S. Hrg. 115–588

EVOLVING THREATS TO THE HOMELAND

HEARING

BEFORE THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

ONE HUNDRED FIFTEENTH CONGRESS

SECOND SESSION

SEPTEMBER 13, 2018

Available via the World Wide Web: http://www.govinfo.gov

Printed for the use of the
Committee on Homeland Security and Governmental Affairs

U.S. GOVERNMENT PUBLISHING OFFICE
34–575 PDF WASHINGTON : 2019

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

RON JOHNSON, Wisconsin, *Chairman*

ROB PORTMAN, Ohio
RAND PAUL, Kentucky
JAMES LANKFORD, Oklahoma
MICHAEL B. ENZI, Wyoming
JOHN HOEVEN, North Dakota
STEVE DAINES, Montana
JON KYL, Arizona

CLAIRE McCASKILL, Missouri
THOMAS R. CARPER, Delaware
HEIDI HEITKAMP, North Dakota
GARY C. PETERS, Michigan
MAGGIE HASSAN, New Hampshire
KAMALA D. HARRIS, California
DOUG JONES, Alabama

Christopher R. Hixon, *Staff Director*
Gabrielle D'Adamo Singer, *Chief Counsel*
Michelle D. Woods, *Senior Professional Staff Member*
Colleen E. Berny, *Professional Staff Member*
William G. Rhodes III, *Fellow*
Margaret E. Daum, *Minority Staff Director*
J. Jackson Eaton, *Minority Senior Counsel*
Subhasri Ramanathan, *Minority Counsel*
Julie G. Klein, *Minority Professional Staff Member*
Laura W. Kilbride, *Chief Clerk*
Thomas J. Spino, *Hearing Clerk*

CONTENTS

WITNESSES

Thursday, September 13, 2018

Alphabetical List of Witnesses

APPENDIX

EVOLVING THREATS TO THE HOMELAND

THURSDAY, SEPTEMBER 13, 2018

U.S. SENATE,
COMMITTEE ON HOMELAND SECURITY
AND GOVERNMENTAL AFFAIRS,
Washington, DC.

The Committee met, pursuant to notice, at 10:31 a.m., in room SD–342, Dirksen Senate Office Building, Hon. Ron Johnson, Chairman of the Committee, presiding.

Present: Senators Johnson, Lankford, McCaskill, Carper, Peters, Hassan, Harris, and Jones.

OPENING STATEMENT OF CHAIRMAN JOHNSON

Chairman JOHNSON. Good morning. This hearing will come to order. I want to thank the witnesses for traveling here, for taking time to write your testimony, and your willingness to appear and answer our questions and give us your oral testimony.

I will ask that my written statement be entered in the record.[1]

As I was explaining out back or in the ante room, this hearing really is borne out of my own personal frustration. I have been here 7½ years, and I cannot remember where this phrase was coined, but it is over the last couple of months as I have been talking about a number of these issues. We have been sitting here admiring these problems and just not effectively addressing them.

So, today, we are not covering all the potential threats. We are going to have our full-fledged threat hearing with the Federal Bureau of Investigation (FBI) Director and Secretary of the Department of Homeland Security (DHS) and the head of the counterterrorism group. That will be in a couple weeks.

But I wanted to assemble some experts on some of these specific threats that literally could be existential. I do not want to scare people. I am always, to a certain extent, reluctant to lay out these threats. I do not want to give people any ideas, but some of these things are just so public now and so obvious in terms of what these problems are.

I think it was in March 2015. We had Joe Lieberman and Tom Ridge here. They developed this blue ribbon study panel on biothreats, and back then, they had a pretty simple suggestion. Number one recommendation was we need somebody in charge. There are more than 20-some different appropriations, different agencies, and a number of different agencies were doing things. But there

[1] The prepared statement of Senator Johnson appears in the Appendix on page 35.

was nobody in charge of what happens if we actually had a real biothreat and how we would react to that.

I would say kind of the same thing is true of cyber. We have Kevin Mandia, a real expert with FireEye, talking about the different types of cyber threats.

It is certainly true with drones. We have been trying to pass a bill—I think we are getting a little bit closer—in terms of just giving DHS the same authority to start studying how to counter and some authority to counter drones, like the Department of Defense (DOD) and the Department of Energy (DOE) has over some of their facilities.

But I was shocked. I think most of my colleagues were shocked that we do not have the authority to even study, much less counter use of drones.

We have held multiple hearings on the threats of Electromagnetic Pulse (EMP) and Geomagnetic Disturbance (GMD), and we have Scott McBride here from the Idaho National Laboratory, a real expert on that subject, both EMP and GMD, but also just electric grids in total as relates to potential cyberattacks or kinetic attacks as it relates to that.

And then we have Jennifer Biscelgie in terms of a strategic resource management, in terms of how do we strategically look at the threats of our supply chain, which has also come up with whether it is Huawei and Zhongxing Telecommunication Equipment (ZTE) and just other threats from that standpoint.

So, again, I just want to thank all the witnesses. I am looking for some practical solutions, things that we can actually do. We have admired this problem enough. We have studied it enough. We have not produced the strategies, and that is true, but I am actually looking for some concrete things we can take away from this hearing. And maybe if there is a law that we have to pass, try and pass that law, but just try and figure out something. Let us do something about some of these problems.

With that, I will turn it over to our Ranking Member, Senator McCaskill.

OPENING STATEMENT OF SENATOR MCCASKILL[1]

Senator MCCASKILL. Thank you, Mr. Chairman.

Two days ago marked the 17th anniversary of the September 11, 2001 (9/11) attacks on this Nation. It is a somber reminder of the threats we face and that we must continue to vigilantly protect the country from those who wish to do us harm.

In the 17 years since 9/11, Congress and the American people have had spirited debates surrounding the nature of threats to the United States and how best to protect ourselves from them.

A lot has changed over these nearly two decades, but until recently, one component remained constant. Since joining the Senate over 30 years ago, my friend and colleague, Senator John McCain, was an integral part of every national security conversation that took place in this body. His commitment to public service, his dedication to the defense of our country, and his efforts to promote American values were unparalleled.

[1] The prepared statement of Senator McCaskill appears in the Appendix on page 37.

I had the privilege of serving with him on this Committee and on the Senate Armed Services Committee. His conviction, insight, and sense of humor will be sorely missed, even his incredible temper. John McCain made an indelible mark on the security of this Nation, and I will miss him as a colleague and a partner in addressing these complicated issues.

I also welcome Senator Kyl back to the Senate and to this Committee, and I look forward to working with him.

The United States has made enormous progress in preventing another 9/11-style attack, but threats to the country remain. Terrorism continues to evolve as a threat and requires innovative solutions to confront and prevent it.

As the United States and the world become more digitally connected and as technology advances at a rapid pace, we have new vulnerabilities. This hearing provides an opportunity for the Committee to focus on some of those concerns and explore real solutions.

In 2013, for the first time, then-Director of National Intelligence James Clapper prioritized cyber threats above terrorism when testifying before Congress. In the years since, the problem has metastasized. The threat of cyberattacks and cyber espionage regularly dominate headlines, and with the midterms approaching, election security is obviously of paramount concern.

This Congress, Senator McCain, as Chairman of the Armed Services Committee, created a Cybersecurity Subcommittee on which I serve, where our focus complements the work of this Committee on identifying cyber threats and strengthening our forces and capabilities.

One area of focus that I am particularly concerned about is Supply Chain Risk Management (SCRM) and specifically the information technology (IT) and telecommunications supply chains within our government agencies and the U.S. infrastructure.

This evolving threat can turn a mundane antivirus software purchase into an unacceptable risk to our national security. We need to make sure our information technology products and services are safe from infiltration, down to the smallest component, and like most national security issues, that requires a strategy and a whole-of-government approach.

Supply chain risk management cannot be achieved piecemeal. In this regard, a threat to one agency is likely a threat to many others.

In June, Senator Lankford and I introduced the Federal Acquisition Supply Chain Security Act to address this critical issue. Few understand this issue better than some of the experts on this panel.

I hope this hearing will provide the Committee, Federal agencies, and the public with a better understanding of how to solve this problem.

Similarly, this Committee has heard from numerous Cabinet officials and experts in the public and private sectors about threats posed by drones.

Chairman Johnson and I introduced legislation that would authorize the Department of Homeland Security and the Department of Justice (DOJ) to conduct limited counter-drone operations for a narrow set of important and prioritized missions. Our bill is just the simple first step in tackling this mounting problem, and we welcome additional thoughts from the witnesses on solutions that might mitigate the threat.

I thank the Chairman for holding this hearing and look forward to the discussion.

Chairman JOHNSON. Thank you, Senator McCaskill.

It is the tradition of this Committee to swear in witnesses, so if you all would stand and raise your right hand. Do you swear the testimony you will give before this Committee will be the truth, the whole truth, and nothing but the truth so help you, God?

Mr. MANDIA. I do.

Ms. LANIER. I do.

Mr. MCBRIDE. I do.

Ms. BISCEGLIE. I do.

Chairman JOHNSON. Please be seated.

Our first witness is Kevin Mandia. Mr. Mandia is the chief executive officer (CEO) of FireEye, a leading global cybersecurity company. Prior to FireEye, he founded the cybersecurity firm Mandiant Corporation. Earlier in his career, Mr. Mandia served in the United States Air Force as a cybercrime investigator. Mr. Mandia.

TESTIMONY OF KEVIN MANDIA,[1] CHIEF EXECUTIVE OFFICER, FIREEYE, INC.

Mr. MANDIA. Thank you, Mr. Chairman, Ranking Member McCaskill, and other Members of the Committee. I appreciate this opportunity to speak to you today about the cyber threats facing our Nation.

Before I begin discussing these cyber threats, I would like to take a moment to extend our condolences to each of you for the loss of your dear friend and colleague, Senator John McCain.

In my testimony today, I intend to discuss the cyber threats to our Nation, what they are, what their impact could be, and what we can do about it.

I have been working in cybersecurity for over 25 years. As the Senator said, I started my career in the Air Force as a computer security officer at the Pentagon. Following that, I was a special agent in the Air Force Office of Special Investigations, investigating computer intrusions into our military networks, and I have the privilege today to serve as the CEO of FireEye.

As I sit here right now, we are responding to dozens of breaches around the world. We have over 300 investigators that conduct over 600 investigations every year into what happened during the breach and what to do about it. We have over 100 threat analysis that are in 18 different countries that speak 32 different languages, actively tracking the threat actors on a global basis to try to get attribution behind who is doing it. And we have over 15,000 sensors that every hour detect between 50 to 70,000 malicious events. We are the last line of defense for computer security for our customers.

[1] The prepared statement of Mr. Mandia appears in the Appendix on page 40.

We have been seeing the attacks firsthand. We know how the attackers are evading our safeguards, and we have witnessed the impact that these attacks have had firsthand as well.

Let me begin by sharing three general observations about the cyber threats to the United States. First, I believe the United States is more vulnerable in cyberspace than other nations. First, we depend more on the Internet, the connectivity, the technology, and the infrastructure than the nations that host the most prevalent cyber attackers, such as Iran, Russia, China, and North Korea.

Second, our critical infrastructure is shared. For the most part, it is in the hands of the private sector, and during times of duress or outright war, if we need to do "shields up" in a joint defense, we are going to need to cooperate between the government and the private sector, whereas many other nations, some of their critical infrastructure is purely government controlled.

Third—and it sounds odd, but it is true—that a weakness of the United States is in fact in cyberspace, freedom of the press, fundamental to our democracies, but it gives attackers two advantages that we simply do not have if we reciprocated those types of attacks on closed societies.

First, influence operations can be conducted in the United States with greater efficacy than in a closed society. Second, the ability to attack an organization or an individual, steal their information, and threaten to publish it online in any capacity; or to threaten or hold their information hostage is an invasion on our privacy. It allows folks to leverage our citizens in ways that closed societies do not need to worry about as much.

The second observation I would like to make is that a lot of people talk about Pearl Harbor scenarios against the Nation in cyberspace. I think what is going to be more likely is what we refer to internally at FireEye as "cyber trench warfare." I want to talk about some of the ingredients for cyber trench warfare.

The first characteristic is that it is going to be conducted below the threshold that would elicit an aggressive response by the United States. It will be low and slow. It will endure, but it will slowly erode our willingness to combat it over time. Second, the campaigns will be long term. Third, these campaigns are going to go after, in my opinion, the softer targets. A lot of people think that critical infrastructure in the military will be target number one if we have a modern war. In fact, it may very well be the softer targets, small municipalities, health care, small elementary schools, the small businesses that make the fabric of our daily businesses run. Those will be the soft targets that are in fact attacked, and in aggregate, if all the soft targets in this country succumb to a destructive attack, the impact and consequence can be pretty grave.

The last general observation that would happen during any cyber conflict against the United States, is what I describe as a butterfly effect, and it works two ways. Whenever there is a cyberattack, when somebody takes the gloves off and escalates in cyberspace, even the perpetrators are not fully aware of what the impact of these attacks will be. If somebody launches an indiscriminate, destructive attack on our Nation, they do not know what unintended consequences can happen from that.

But I do know this. We have not been able to predict it either, and imagine if the U.S. Senate came offline for a day or two from the Internet, what would happen? Would you be able to get into the parking garage? Would you be able to even make a phone call from your desk? Would you be able to buy lunch in the cafeteria downstairs? It has a lot of unintended consequences that people have not predicted in the past.

So what do we do about it? The threats to our Nation are growing. I gave you some high-level observations about this, but by establishing a system where the private and public sectors work together, we practice together. That is key. We practice together doing dry runs, and we proactively use threat intelligence. We can create a learning system. We are getting better every day, but we can accelerate getting better at a faster rate.

And, last, we need to explore international rules of engagement and hold threat actors accountable. Right now, the key word is "deterrence." Do we have a deterrence against cyber-threat actors against our Nation? What can we do about that?

If we find a way to have some diplomatic treaties or agreements with other nations that are launching these attacks, the United States and the daily lives of our citizens will be better safeguarded.

Thank you, Mr. Chairman.

Chairman JOHNSON. Thank you, Mr. Mandia.

Our next witness is Cathy Lanier. Ms. Lanier is the senior vice president of Security for the National Football League (NFL). She previously served as the Chief of the Metropolitan Police Department of the District of Columbia. Ms. Lanier.

TESTIMONY OF CATHY LANIER,[1] SENIOR VICE PRESIDENT OF SECURITY, NATIONAL FOOTBALL LEAGUE

Ms. LANIER. Hi. Good morning, Chairman Johnson and Senator McCaskill. How are you? Members of the Committee. Thank you again for the opportunity to testify here today.

As requested, I will focus my testimony on the threat posed by malicious drones at major sporting events.

At the NFL, we have observed a dramatic increase in the number of threats, incidents, and incursions by drones. Fewer than 10 miles from here, a drone flew over FedEx Field during pregame activities for a Monday Night Football game, violating Washington's national security airspace and the airspace restrictions of the NFL game.

The NFL is not alone. For example, in 2017, a drone crashed into the stands of a Major League Baseball game between the Padres and the Diamondbacks.

A 2017 incident involving two NFL stadiums dramatically demonstrates this threat. During a San Francisco 49ers game, the stadium security director at Levi's Stadium called me and alerted me that a drone had just dropped leaflets over the seating bowl. I warned the other teams, so when the operator sought to fly a drone over nearby Oakland Coliseum, local law enforcement was ready for them. They were able to quickly identify the operator and arrest him.

[1] The prepared statement of Ms. Lanier appears in the Appendix on page 46.

We are all very fortunate that the drone over Levi's Stadium dropped just leaflets. Drones today are capable of inflicting much greater damage.

As the Committee knows, various threat assessments have recognized that large gatherings of people are enticing targets for malicious actors.

The Federal Aviation Administration (FAA) and Congress have therefore imposed flight restrictions on the airspace above large sporting events. The FAA first established these restrictions after 9/11, and Congress subsequently strengthened and codified those requirements.

The current temporary flight restrictions prohibits aircraft over NFL games, Major League Baseball games, National Collegiate Athletic Association (NCAA) Division One football games, and major motor speedway events such as National Association for Stock Car Auto Racing (NASCAR). These flight restrictions have largely worked as intended, keeping commercial and civil aircraft away from stadiums during games. Drones, however, present an entirely different challenge that needs an appropriate legislative response.

Drones can be acquired easily and cheaply. They are often used by unlicensed individuals, with no awareness of airspace rules, flight restrictions, or many other regulatory requirements related to aircraft.

Stopping drones is currently extremely challenging. Drones are small and portable. They can be launched quickly and very close to a stadium from an adjacent parking lot. Several stadium security directors have told me that they are regularly approached by vendors selling counter-drone equipment. They know that using such devices are illegal.

The current State of law, however, leaves security officials with an unenviable choice: Procure the equipment whose use would be illegal, or remain unequipped to respond to a security threat that can endanger tens of thousands of people.

The NFL, therefore, supports the development of new approaches to drones. We support the FAA's remote identification effort. We support revising the hobbyist exemption, which currently permits far too many drones to be flown by far too many unlicensed and untrained pilots.

Further, we support the aim of your legislation to extend drone interdicting authority to DOJ and DHS. Your bill is an important step forward.

In particular, the bill permits State officials to request Federal support for local law enforcement efforts. The bill correctly recognizes that local law enforcement officers are primarily responsible for security at locations where drones present risks such as NFL games.

Although this provision permits local officials to request Federal assistance, there is not enough Federal resources to provide security at all the events that need protection, including the 256 NFL games in a season.

The NFL, therefore, strongly encourages Congress to consider additional reforms that would provide authorities to local law enforcement officers to detect and intercept drones that pose a threat to major sporting events like our NFL games.

The NFL looks forward to continuing to work with Congress, the FAA, and others on our shared goal of ensuring the safety and security of our players, coaches, fans, and staff that attend our games.

Thank you so much for the opportunity to be here today. I appreciate your time.

Chairman JOHNSON. Thank you, Ms. Lanier.

Next witness is Scott McBride. Mr. McBride is the Infrastructure Security Department manager within the National and Homeland Security Infrastructure Protection Department at Idaho National Laboratory. Mr. McBride directs power systems engineering projects for the lab's clients, including the Department of Energy and Department of Defense. Mr. McBride.

TESTIMONY OF SCOTT MCBRIDE,[1] MANAGER, INFRASTRUCTURE SECURITY DEPARTMENT, IDAHO NATIONAL LABORATORY

Mr. MCBRIDE. Thank you, Chairman Johnson, Ranking Member McCaskill, and distinguished Members of the Committee for holding this hearing and inviting Idaho National Laboratory's testimony on the potential threat of geomagnetic disturbance and electromagnetic pulse to the U.S. power grid.

At Idaho Nation Laboratory, I manage power system projects, industrial control system security to secure critical infrastructure throughout our Nation, with a primary focus on the energy grid.

As the U.S. electric power grid incorporates new digital technology with decades-old infrastructure, the grid is becoming vulnerable to GMD and EMP events, whether the EMP source is from nuclear or non-nuclear sources. We have developed a fairly robust understanding of the scientific principles of the damaging waveforms associated with GMD that enables us to predict effects and design protections to mitigate those effects.

Initial experiments have been completed, and models are beginning to emerge that assist us in better understanding and characterizing effects and impacts from the individual waveform specifically associated with an electromagnetic pulse.

Research and testing of the interdependent effects of the combined three waveforms on our grid's individual components and interconnected infrastructure is an uncharacterized field of study that needs further exploration and discovery.

There are ways the United States may improve its understanding of the extent of the vulnerability and reduce or eliminate consequences of GMD and EMP events.

In addressing this need, the Department of Energy recently tasked the National Laboratories to develop a report that updates the extent of our current scientific understanding of the effects of EMP on the electric power grid. Pending this report's publication, significant progress for GMD and EMP grid protection can be made by pursuing four concurrent paths.

[1] The prepared statement of Mr. McBride appears in the Appendix on page 51.

The first adopts EMP hardened transformer neutral blocking devices designed to provide automatic protection for transformers against GMD events to prevent harmonic generation, reduce reactive power demand, and reduce voltage collapse.

The second defines the EMP threat environment, including research coupled currents and voltages for transmission and distribution lines, in support of developing an informed all-hazards protective strategy.

The third conducts a series of scaled experiments on a variety of grid components and restoration assets to understand, predict, and measure the impacts of EMP events on unprotected systems as well as the effectiveness of protective options.

The fourth identifies the prioritized infrastructure that can lead to a most effective and impactful set of actions that will harden the grid and enable reliable black-start processes.

Following this research path with appropriate and coordinated government and industry partnerships can lead to a set of effective hardness and protective measures for GMD and EMP events that add quantifiable, cost-effective resiliency to the power grid.

Current gaps in knowledge suggest that the experiments of highest priority would include assessing the damage from integration of the propagating electromagnetic radiation effects to grid assets directly connected to long power lines, antennas, and communication and data lines; measuring effectiveness of shielding, including nonconductive critical communication fiber-optic cables, well-grounded equipment racks, and shielded buildings, such as power grid control centers; determining the effectiveness of developmental technologies for transient voltage surge suppression; and finally, exercising high-voltage system operations and processes for critical systems spares replacement, restoration procedures, and recovery processes.

This research will have the most benefit if the results are concurrently shared with stakeholders who are developing priorities for more research that can be utilized to enhance predictive models and provide stakeholders with the sound technical basis for standards and regulatory guidance. While it may not be plausible to protect all assets, careful prioritization of the research and implementation of protections can enable critical portions of the grid to survive or at least be rapidly restored following a GMD or EMP event.

Cooperation between government and industry can accelerate full implementation of a protection strategy through a greater technical understanding of GMD and EMP threat characteristics and system effects.

Thank you.

Chairman JOHNSON. Thank you, Mr. McBride.

Our final witness is Jennifer Bisceglie. Close enough. You can tell us what it is. [Laughter.]

Ms. Bisceglie is the president and CEO of Interos Solutions, Inc., which assists public and commercial sector customers with supply chain and vendor risk management. Ms. Bisceglie is named the AT&T Innovator of the Year in 2015.

TESTIMONY OF JENNIFER BISCEGLIE,[1] PRESIDENT AND CHIEF EXECUTIVE OFFICER, INTEROS SOLUTIONS, INC.

Ms. BISCEGLIE. Chairman Johnson, Ranking Member McCaskill, and Members of the Committee, thank you for the invitation and the opportunity to speak with you today on the underappreciated threats to the homeland that, if not mitigated, could significantly damage the Nation's critical infrastructure and/or disrupt people's lives, especially as it relates to the global supply chain and the use of information and communications technology (ICT).

By way of introduction, Interos is a company I founded over 13 years ago to evaluate the risks in the global economy and our business partnerships, alliances, and distribution networks that comprise our supply chains.

The company is built on my over 25 years in the global supply chain industry, having helped multiple U.S.-based companies create maximum advantage from different skillsets, labor pools, and competitive business arrangements with partners around the world.

During those years, I have watched risk concerns in the supply chain move from quality to physical security to resiliency and now product integrity and the role of the digital connection or cyber.

Published in April of this year, Interos' report for the U.S.-China Economic and Security Review Commission for supply chain vulnerabilities when sourcing technology specifically from China and using that technology in the U.S. Federal IT networks stressed several solutions, the most important being that the United States establish a national strategy for supply chain risk management in U.S. ICT with supporting policies, so that the Nation's security posture is forward-leaning versus reactive and based on incident response.

Our adversaries are very public about executing a strategy against us. The time has come for us to stand strong and visibly protect ourselves.

In my submitted testimony, I spoke to six areas that are directly related to today's hearing. I will be summarizing them here for this briefing, with focus on three, and I have been massively updating the last one based on your pep talk—and then open the remaining time for any questions you have.

Before addressing the specific areas of the report, I would like to stress that whether it is 5G or blockchain, the Internet of Things (IOT), or any other emerging technology or technological threat, an underlying foundation for security, both physical and digital, is an understanding of who the stakeholders are, where your vulnerabilities lie, and having a strategy for managing those associated risks.

The solution cannot solely be focused on the latest tools and technologies. Cultures need to change. The money needs to be spent to educate people on their role in traditional risk management.

Given our position in the market, my company has had the opportunity to work with public and private sector organizations, spanning multiple industry verticals. In the government, we have worked with Defense Intelligence Agency (DIA), National Security

[1] The prepared statement of Ms. Bisceglie appears in the Appendix on page 57

Agency (NSA), several Office of the Secretary of Defense (OSD) members, the General Services Administration (GSA), Social Security Administration (SSA), Federal Deposit Insurance Corporation (FDIC), Department of Energy, and the National Nuclear Security Administration (NNSA).

In the private sector, we have worked with manufacturers, the financial institutions, utilities, and others, and the situation is always the same. If the organization does not take a focused and comprehensive approach to risk management prioritized by senior leadership, there will be unnecessary exposure and invariably negative impact.

We would also like to stress that the supply chain attacks will continue to become easier, more prevalent and more threatening as emerging technologies, such as the one I mentioned earlier with 5G, the Internet of Things, and others increase the attack surface exponentially.

As a point of clarification, just briefly, you will hear the term SCRM a lot.

Very quickly in the time that I have left, how reliant is the U.S. Government and U.S. IT firms specifically on China firms and Chinese-made IT products and services? The answers vary. Over 95 percent of our electronic components and IT systems supporting the U.S. Federal IT networks and commercial off-the-shelf products come from China. They have done this on purpose. It is an economic movement, and that is just where all the sourcing comes from.

Number two, to assess the government success in managing these risks associated with the sensitive country firms and sensitive country-made products, in short, there is very little systemic success, and that is part of the reason we are having this conversation today.

And I think the last part is what steps should we take, and this goes back to the conversation earlier. I have changed my comments. They will align with what I submitted, but six very specific things, if I were to leave this room today, the first is—and the act that we talked about earlier brought it up—a single whole-of-government approach that the Department of Defense and other agencies cannot self-elect out of. We are all using the same suppliers, and there has to be some sort of exception management process because things do pop up, but there really just needs to be a single risk-management approach for the government.

There really needs to be somebody in charge, and the person needs to report to the head of the agency. And it cannot be a political person. This is not a political problem. It is a business problem. We cannot keep changing people as the Administration changes. You are never going to get ahead of it.

The third, you need to have a line item resource for the agencies to use. Right now, the way that this is managed across the intelligence community (IC), the DOD, and the civilian agencies, it is robbing Peter to pay Paul. There is no money associated to supply chain risk management in the agencies.

The fourth—and the act does talk on this—is a real partnership with industry. We need to fix the Federal Acquisition Regulation (FAR). We need to fix the Defense Federal Acquisition Regulations

(DFARs), the Defense Enrollment Eligibility Reporting System (DEERS), and any other acquisition strategy we have in the government. The National Institute of Standards and Technology (NIST) has a role, but it is as an evangelist and a supporter. They are not a leader in this conversation. They do not dictate how business operates. This is a business problem.

The second to last is metrics on the impact, not just activity, not just how much money did we spend or what are we doing, but specifically what mitigations, what problems with mitigations and how did we share that information to get better as the whole of government. And I think, again, the act can help with that.

And then the last part is not to overclassify this problem. That is a problem I run into in every agency, and the thing that we have to remember is that this is a global business and economic issue, and every time we overclassify it, we reduce the amount of people that can have an impact on solving the problem.

So, with that, I will turn it back. Thank you.

Chairman JOHNSON. Thank you.

I am going to reserve my time out of respect for my colleagues' time, but one of the big problems in just about every one of these situations is the complexity of the problem. The expert witnesses, you speak in language that laymen do not understand. Again, I really appreciate your expertise, and we need it in your written testimony, to answer our questions, if you could, as much as possible try and convey this in layman's terms. It would be very helpful.

One of the analogies I use is I am old enough to remember "Gilligan's Island," and on this island, most of us are Gilligans. Not too many professors know how to turn a coconut into a battery.

I do not care whether it is cyber, whether it is EMP, whether it is encountering drones. This is incredibly complex technology and just science, and that is part of the problem the government has in dealing with these problems, is nobody understands it in the agencies or in Congress. So that is a hurdle I am just really not quite sure how we are going to ever overcome.

But, with that, I will turn it over to Senator McCaskill.

Senator MCCASKILL. I want to talk a minute about supply chain. I would like your take on this, Ms. Bisceglie and even Mr. Mandia.

I read in the morning paper and what really concerned me is the conflict we have going on now in Turkey. We reached out to eight nations to help us build the F–35, including Turkey. Turkey is building—a cockpit display—is one of their companies, defense contractors, and a center fuselage.

Well, now we have Erdogan in disagreement with the United States. So he has now decided he is going to go buy the Russian air defense system, S–400 from Russia, instead of working with us to acquire the Patriot.

So now we have this bizarre situation; Russia, who we know has conducted cyber warfare against our country, is beginning to put an air defense system in the same country that is building the cockpit displays and the center fuselage on our next generation fighter pilot.

Should I be worried about this? Ms. Bisceglie.

[Speaking off microphone.]

Senator MCCASKILL. Absolutely.

Ms. BISCEGLIE. We are actually talking to the F–35 program as well.

And back to the Senator's comment, to me—and maybe I am very simple about this, but this—again, it is a business problem. And so we are actually working with a very large technology company right now around prototyping, and I will bring it back to exactly what you asked about, but the whole idea is getting out of the fact that we are in a world that there is only a single source of supply. There is not.

There is either other companies that can be competitive that are today competitive or other companies that if we put research and development (R&D) dollars into them could be competitive. So they do the 75 percent solution; they need the 25 percent to develop.

And so with this technology company, that is literally what we are doing around prototyping, is figuring out what are the products and the components and the software that they are going to need in the near and the long term, and how do we look globally at where suppliers exist in the world in places that maybe we do not want to deal with and we do have to deal with them because of cost, because of time that I need that product or service, or other places in the world that are a bit more friendly to how I do business? And then I can start developing it, so I have multiple sources of supply. So I do not have a situation that you are talking about right now.

Senator MCCASKILL. Except the problem is with this, the reason they did this is they wanted to bring down the cost by having more orders.

Ms. BISCEGLIE. Right.

Senator MCCASKILL. So this was a quid pro quo. We are going to give you pieces of the production in return for an order for 100 F–35s because the more we build, the cheaper they get.

So that to me is the challenge here, is that we are doing business with a very sensitive part in an incredibly important weapon system with a country that is now playing footsie with our cyber enemy.

Ms. BISCEGLIE. Right. I think it goes back to my comments earlier, and again, ma'am, maybe I am doing this too simply, but to me, this is very much a business situation and it is risk management that says I am willing to deal with that sensitive country because of cost or I am going to pay a little bit over here, more over here, because I do not want to deal with that country. And if we could get out of the politics, understanding that is part of risk management——

Senator MCCASKILL. Right.

Ms. BISCEGLIE [continuing]. And say, "You know what? I am willing to accept this risk over here, and I am going to mitigate more on my side," that is a risk management approach.

What you are talking about is exactly the conversations we are not having. We are just saying "China bad" or "Turkey bad," and that is just not the world we live in.

The more that our leadership that is actually involved in these programs is focused on this is what I can deal with from a risk standpoint and this is what I cannot and focus on requirements, I honestly think that—businesses have been doing this forever. This is really how business is done. We cannot get excited over the political aspect. I actually think that is to our detriment.

Senator MCCASKILL. Well, business and the Pentagon are sometimes two mutually exclusive concepts——

Ms. BISCEGLIE. Yes, ma'am.

Senator MCCASKILL [continuing]. Let me just say, having done a lot of work on contracting in the Pentagon.

Do you have anything you would like to add to that, Mr. Mandia?

Mr. MANDIA. Yes. I think at the highest level of abstraction, Senator, economics follows geopolitical conditions. Cyberattacks are directly linked to geopolitical conditions. Security is related to it.

When I listened to what you were saying, it dawned on me that the exact same challenges we have with Turkey building very important components and essential components to anything, we have the same problem here in the United States. We have small companies that cannot protect themselves in cyberspace——

Senator MCCASKILL. Right.

Mr. MANDIA [continuing]. But they are building mission-critical systems.

Senator MCCASKILL. Exactly.

Mr. MANDIA. So, obviously, as part of the process, we have to build security in it and checks and balances into the process, regardless of where construction and where the supply chain resides.

Senator MCCASKILL. Have either one of you had a chance to look at the supply chain risk management bill that Senator Lankford and I have introduced? It is very similar to a proposal the White House has made. Is there any input you would like to have on that legislation?

Ms. BISCEGLIE. So I have, and actually, if I had kept to my original comments, I think it is a very good start.

I think when I first heard about it, it heartened me, having been in this industry for so long, that we have raised the visibility up to this level.

I think that my comments—and I have been asked to submit as well—is that from an implementation standpoint—and I understand it is the first time we have gotten the conversation to this level—I still do not think we have enough industry and business involvement because, at the end of the day, that is who is actually going to execute against it.

So the players that are included in that bill are all the normal players from a government standpoint, but I would like to see more direct industry involvement, which is not necessarily just through trade associations, but specialties in different industry sectors, which I think from an implementation standpoint will make it more impactful from an implementation as well as reduce the cost.

Senator MCCASKILL. I am going to turn to another subject now. If you have anything else on this, Mr. Mandia, I would sure like you to submit it.

So what happens if the folks at Busch Stadium in St. Louis get information that there is going to be a drone incursion, and that their sources tell them—maybe it is the St. Louis police department—that it is an armed drone.

So if that were to occur today, what would happen to the Cardinal organization if they took it down? What penalties would lie against the Cardinal security operation if they actually took down that drone?

Ms. LANIER. So it would depend. First of all, we typically would not get intelligence or information that a drone is incoming, but if we did and if there was mitigation or interception technology available and that was used as one of several different types of technologies, it would be illegal for them to use that to take that drone down.

Senator MCCASKILL. What would happen to them? What are the penalties? Do you know?

Ms. LANIER. I cannot tell you the penalties. It just depends on which type of——

Senator MCCASKILL. Well, can I just tell you that I will represent them for free if they take it down?

Ms. LANIER. I will pass that along.

Senator MCCASKILL. Ultimately at the end of our processes in law, there is a jury, and juries are very good about weighing the facts. If you let juries decide things, they very—I mean, not that they do not make mistakes, but a jury in that circumstance, I can assure you would apply common sense and say this was a matter of risk management, and what they did was the right thing.

We are going to rush to get something done. We are trying to get something done that would give people the authority to take action in those circumstances, but it scares the bejesus out of me that——

Ms. LANIER. Unfortunately, this is a discussion that is going on, and it should not have to go on. You have people that want to make sure they are providing adequate security and safety for 70 or 80,000 people, and they want to do the right thing. Nobody wants to be at odds with the law under any circumstance.

Senator MCCASKILL. Right.

Ms. LANIER. So that is the discussion that goes on, quite honestly.

Senator MCCASKILL. Well, I just think that, obviously, if you are faced with a dilemma of the unknown being harm to thousands of people versus the unknown of what happens to us if we do it, I just want to encourage them to use common sense.

Chairman JOHNSON. Of course, one of the problems right now is DHS does not even have the authority to study how to knock that thing down. It is a problem.

Again, if they knock down malign drones, my guess, the jury would rule correctly. The problem is, What if they knocked down the wrong one in good faith? Then they would have greater liability, and that is what we are trying to give. We are trying to give them the liability against that type of event. Senator Hassan.

OPENING STATEMENT OF SENATOR HASSAN

Senator HASSAN. Thank you, Mr. Chair and Ranking Member McCaskill, and add me to the group that would call for the application of common sense here when it comes to protecting people at large events.

I wanted to focus with you, Mr. Mandia, on some of the issues that come up with small vendors and cyber threats. In your testimony, you spoke about the challenges that smaller companies and organizations face from cyber threats. In particular, you pointed out that their vulnerabilities not only threaten their operations but their partners, their customers, their suppliers, and ultimately our country's economy.

Your point underscores the importance of making sure that the Federal Government does all it can to help protect these small companies and service providers.

Last spring, DHS revealed that Russia targeted several small vendors through a cyberattack to gain access to our electric grid. DHS reported that many of these vendors lack the resources or dedicated cybersecurity professionals to detect and prevent these kinds of intrusions. It does not seem reasonable to me to expect companies with only a few staff and maybe one full-time IT professional to be able to defend against the fully offensive cyber capabilities of State-level cyber actors like Russia.

What should be DHS's role in helping to secure these companies, and what sort of resources should we be considering in order to achieve some degree of defense against State-level hacking?

Mr. MANDIA. You have to take this in a couple parts. Great question, one of great concern to many people.

First and foremost, if all we do is play defense, if we are up against Russia, we are up against Wayne Gretzky on a penalty shot, and we have a bunch of goalies out there, where if they get unlimited penalty shots, they are going to put the puck in the net.

What I have observed in the private sector in practice is the bigs are helping secure the "smalls" and taking on some of the burden of doing that, but we cannot win if all we do is focus on defense, defense, defense. And that is why we need to have imposed risks and consequences to those who do it, which means we have to get attribution rights support the technical assets, the human assets, the international cooperation so that we know who is doing these attacks——

Senator HASSAN. Right.

Mr. MANDIA [continuing]. So we can at least weigh a proportional response to it.

But when we also look at it, we have to take it in bite sizes. We cannot secure every company overnight, all the "smalls". You have to start with the ones in the critical infrastructures, and I believe if you can secure the "bigs" first, the "bigs" will help you secure the "smalls", and you start with the utilities. You start with health care. You start with communications. And you work that way.

I think you have to take it industry by industry. If you protect the company, then you can protect the industry, and if you protect certain industries, you can protect the Nation.

There are three ways to slice it, but we are certainly going to need some deterrence to come to the table.

Senator HASSAN. Well, I thank you for that response, and we will likely follow up with you on it some more.

I wanted to move now to the issue of Federal network security. According to your testimony, FireEye has worked closely with DHS and dozens of civilian and Federal agencies to provide these agencies with the capabilities needed to achieve a baseline of security against cyber threats.

As we see increasingly more sophisticated and diverse cyberattacks, DHS's role in helping to protect Federal agencies and the dot-gov domain from cyber intrusion will become all the more important.

To that end, DHS has endeavored to strengthen the tools and capabilities it provides to Federal agencies to protect themselves, including the maturation of its two signature programs, the EINSTEIN Program and the Continuous Diagnosis and Mitigation Program. Can you please talk to us about the value of these programs in enhancing Federal network security and how they may need to evolve in order to keep pace with a really diverse and ever changing threat, a cyber-threat environment?

Mr. MANDIA. Yes, I can, and I will make it brief.

You have to start somewhere I was a big proponent of the EINSTEIN stack because it sets the floor of how good you are, and you know what you are working with. If you can have a referenced architecture, it is easier to manage.

We have a shortage of security professionals. You do not want to learn 180 different products. You need to keep it down to the five to eight that are best of breed at that moment, but you also have to create a learning system. And that is where the intelligence comes in.

At the highest level of abstraction, I have been working with the government since 1993 in cybersecurity. We are getting better every year, so that is the good news.

Senator HASSAN. Yes. Well, thank you for that.

Let me follow up with one last topic on the issue of cybersecurity generally, which is something you have talked about, cyber resiliency.

You mentioned it in your testimony that one of the best ways to counter the threat of a crippling cyberattack is to mitigate the effects of such an attack through strengthening private and public sector cyber resilience.

You gave the example of how an Alaskan-based company worked to survive a ransomware attack by reverting to typewriters and handwritten notes to maintain daily operations.

While I was Governor, we worked to develop continuity of operations plans for our State agencies and government, and that included considering how to access data and how we would operate without technology.

Obviously, in an ideal world, we want to avoid bringing out carbon paper again, right? But can you help us identify the best ways to achieve effective cyber resiliency? What sort of mechanism and incentives would need to be put in place to encourage the private sector to develop this kind of resiliency, and what can the U.S. Government's role be in helping to achieve baseline cyber resiliency?

Mr. MANDIA. Yes. I think it is a great question.

Bottom line is life fire drills. The only way you are ever going to get better at something is if you force the issue, and you keep it—maybe it is utilities and energy first, health care, telecommunications. Financial services are pretty good on their own.

But if you think about it, if the gloves came off in a modern warfare today, what are the two top targets? It is going to be energy; it is going to be telecommunications. And that is where they are mostly in the hands of the private sector. So you have to do a joint drill, and they already are doing this, but is it the only way to get the unvarnished truth that every CEO is operating on. We are as secure as we can get. Even CEOs want the live fire drills, and the red teaming exercise to see what can happen. Then if you coordinate it, it would be a 1-day or 2-day event every year, where you had the private sector and public sector do a joint drill, that simple, and that will give us both, A, how good are we to get the unvarnished truth, and B, so what do we do and how do we operate through it. We will learn a lot just by practicing.

Senator HASSAN. Well, I thank you for that answer, and I think it also speaks to the need not only to prioritize it in concept, but prioritize it in terms of resources because in my experience, if you do not assign that kind of coordination and practice as a priority and devote resources to it, it always gets pushed aside with the urgency of everyday operations. And so we need to really focus on it.

I thank you for your expertise and your help.

Chairman JOHNSON. Senator Jones.

OPENING STATEMENT OF SENATOR JONES

Senator JONES. Thank you, Mr. Chairman, and thank you to all the witnesses for being here today. It is really informative for us.

Ms. Bisceglie, I would like to ask you a little bit more about the supply chain.

I had lunch with a friend of mine in Mobile the other day whose company ships all over the world. They are in ports all over. We talk about the supply chain. We talk about infecting the supplies and those kind of things, as Ranking Member McCaskill said a minute ago. But to me, it is also a problem with the shippers, that those could get hacked. And you divert or either destroy shipments going across, and I would like for you to address that just a moment because the public-private partnerships seems to me very important with folks like that to be able to work with the government to try to minimize those potential attacks. I would like you to address that.

Also, when you were giving us your list of things to be done, you warned against overclassifying the problem, and I would like for you to just dive into that just a little bit more for the record to explain what you meant by overclassifying which I think government often tends to do.

Ms. BISCEGLIE. Thank you for both those questions.

So your point about the delivery mechanisms, to me, that is part of the supply chain. When we talk in the industry, we talk about sub-tiers, and it is one thing I do not think, to the point you are making—in the government, we are not thinking that way yet, so again, back to the act that is being created—the bill that is out there.

The more that we start talking about all of the levels of the supply chain, which is not just the people producing widgets but how those widgets move to the next step, I think it is incredibly important. And when you talk about widgets moving to the next step—and I do not care if that is software or hardware—that is the physical delivery, so the boats and trains and automobiles and all the people involved in that. It is the electronic. It is the blockchain updates. It is the Electronic Data interchange (EDI). It is however you are sending that information, open source software, but it is all of those mechanisms.

So if I were to just take a quick example, if I was to make this pen, so I am the holder of the pen, somebody behind me cobbled that together. I bought it at Staples. Somebody behind Staples cobbled it together. Then you explode the pieces, and in between all of those it was mailed, right? Was it put on a truck? And who are all those people? Humans involved in all of that. To me, that is the multi-tiered supply chain.

We do visualizations of those types of relationships at Interos in my company, and we just did this for one of the topid banks, the top 10 banks in the country. And when they saw how interconnected they were with their suppliers—and not just who they thought they were directly connected to, but how that same company was actually a tier 2 and a tier 3 and, to your point, delivery partners, they had no idea.

So, to me, the more that we as a government partner with industry and think of all of the sub-tiers and all of the hands that touch it, that is really the only way to solve this problem. So it is expanding that definition.

The second thing on the overclassifying is that we do this because we do not understand, and part of what we do not understand is that this is a business problem that needs to be solved. And the second piece is that most businesses do not have the clearances because they do not need the clearances to actually get the job done.

Back to the Senator's point, the more that we can kind of dumb this down and talk about it just business to business, put it into requirements, and so the Senator's point, a lot of the small and medium size businesses, the more you put these things into requirements and say as part of your contract, you have to do X, Y, Z, the better off we are going to be. And classification does not come into that.

Most of the people that actually have to take actions and provide solutions do not have clearances.

Senator JONES. All right. Thank you.

Ms. Lanier, you said something in response to Senator McCaskill's question that struck me a little bit because, obviously, the drone issue concerns everyone. Alabama, my State, has a lot of outdoor events, whether it is the music festivals, whether it is the sporting events. We are in the fall, and college football is a really big deal right now. In fact, many people would think that Alabama should be in the NFL rather than the NCAA, but we will not go there.

But you mentioned that you might not have any notice about an incoming drone, unlike our missile defense system or something like that. Would you talk about that a little bit more and what can we do now to maybe at least get that on the radar, so to speak, a lot of people want to take a picture over Bryant-Denny Stadium when it is full. I get that, but they should not.

What can we do right now to maybe help in that aspect to just put people on notice? Is there something we have the tools with now?

Ms. LANIER. Well, there are efforts under way to try and educate people. A lot of it is people that are just not educated that there are flight restrictions that prohibit the use of drones over most of these large events, like the NFL stadiums on game days. So getting that message out has been a huge effort to try and educate folks.

And there are detection systems. So the technology that is there now comes into two different sets. There is detection capabilities, and then there is interdiction capabilities. Some of the technology that is available—and, again, mostly illegal to use—can detect that a drone is incoming.

A lot of times, they are launched from a parking lot right near or very close by.

Senator JONES. Right.

Ms. LANIER. So there is not a lot of lead time, not a lot of advanced warning that they are coming. So the detection systems would be one thing, but the interdiction systems is the other part of that. And that is kind of what we have been talking about here today, is the ability for someone to have the authority to use that, from a law enforcement perspective to use that technology to intercept that incoming drone so that it does not make its way into the stadium, into the seating bowl where all of those thousands of people are gathering.

Senator JONES. The restrictions that are currently in effect, I think—and maybe I am wrong about this, but as I understand it, there are restrictions about flying a drone within 3 miles of any event that is holding 30,000 or more people. Is that correct?

Ms. LANIER. That is correct, and that is the one that is more difficult to educate people on because it is a temporary flight restriction.

So there have been some measures put in place to geo-fence areas around airports, so that drones cannot go into those restricted areas, but the temporary flight restriction that goes along with mass gatherings, with that threshold and higher, is much more difficult to educate and is not as easily programmable into drones.

Senator JONES. OK. All right. That is all.

I may have some questions for the record, Mr. Chairman. Thank you very much for having this hearing.

Senator JOHNSON. Thanks, Senator Jones.

I do want to underscore the importance of public awareness. It is one of the reasons we are holding this hearing to make the public aware that we have these threats, whether it is the flight restrictions, public exposure in terms of the hacking, whether it is Kaspersky Labs. I think public exposure is extremely important when it comes to cyber defenses. Just people's awareness so they can start looking at their own vulnerabilities is incredibly important. Senator Peters.

OPENING STATEMENT OF SENATOR PETERS

Senator PETERS. Thank you, Mr. Chairman.

Thank you to each of our witnesses for your testimony here today.

While we meet today to talk about the evolving threats to the homeland and look at major threats like cyberattacks, electromagnetic pulses, and drones, I would like to express my concerns about the broader issue of crisis response under our current Administration.

I was disturbed this morning to see that the President took to Twitter to make false claims about the death count in Puerto Rico, which comes days after he claimed the government's response to Maria deserved an A plus.

Nearly 3,000 Americans died as a result of Hurricane Maria and the inadequate response that followed, and yet the President does not accept those results and denies any responsibility for the failures in 2017.

3,000 deaths is not a number invented to attack the President, as he claims. It is the acknowledgement of real human lives. Each number represents a person that trusted in their government to help them in their time of need. Hurricane Maria was devastating, and our country will continue to face evolving threats from a variety of hazards, manmade as well as natural.

Americans should not have to worry that in a time of crisis, a true national emergency, that our commander in chief would cast doubt on very real, very human impacts of the crisis.

And as Hurricane Florence now bears down on the Carolinas, we have to make every effort to ensure that the Federal Government is well-positioned to support everybody in its path, but we cannot forget about the continuing crisis in Puerto Rico and the systemic challenges that led to the horrifying death count that the President today denied on Twitter.

Our Committee or the Federal Spending Oversight and Emergency Management (FSO) Subcommittee should make use of the broad jurisdiction of the Department and governmentwide emergency response to exert strong oversight and hold officials accountable.

Mr. Chairman, I think we should hold a hearing on the failures and lessons learned from the responses to Hurricanes Harvey, Irma, and Maria and hope that we can have a dedicated hearing on that issue.

Chairman JOHNSON. Right now, we have a different subject.

Senator PETERS. I know, but this is of critical importance. And I would hope that we would do that. We were trying to do this in the Subcommittee, and we were informed that the Administrator does not go to a Subcommittee even charged with oversight of Federal Emergency Management Agency (FEMA). We would hope to have your help in getting the Administrator here to answer questions.

Chairman JOHNSON. OK. I would like FEMA right now to concentrate on the hurricane season currently, but we will look at that.

Senator PETERS. I appreciate that, Mr. Chairman.

Certainly, cybersecurity, which is our issue that we are here today to discuss, is a vital component of all of our critical infrastructure. Mr. Mandia, do you put in that category chemical facilities or ones that are potentially susceptible to significant cyberattack and could present a risk to critical infrastructure?

Mr. MANDIA. Yes. I do not know if I can speak to the specifics of all the chemical facilities out there and their cybersecurity posture in defense, so no.

In my prepared remarks, I did talk about indiscriminate attacks, and certainly, every single individual and every single organization, should the gloves come off in cyberspace and there is an escalation, we are all going to get targeted. That is the interesting thing about cyberspace. It is infinitely scalable and can go broad.

A lot of times, the individualized security of one organization in that industry, is only going to be as secure as the weakest link in that industry.

Senator PETERS. Well, I raise the issue of chemical facilities because I have heard that inspectors in the Chemical Facility, Anti-Terrorism Standards (CFATS) Program, who mostly have physical security backgrounds, they are worried that they do not have the appropriate knowledge and training to assess whether or not the facility owners have appropriately addressed the risk to cybersecurity.

So my question to you is, How can we get these folks the training that they need, and certainly fits into their very busy schedule now in order to be able to supervise these activities?

Mr. MANDIA. I can tell you, speaking generically, as a public CEO, you never want to see more and more regulation. The reality is regulated industries, generally, at least you can set the benchmark or threshold for what security they will have, and if it is important enough to the Nation to secure those types of organizations that create certain chemicals, you could regulate them. You could find a way to do a benchmark of security that they have to have. And once that is the case, there are plenty of opportunities to hire cybersecurity professionals. There is plenty of training that they can obtain.

And we saw work in the private sector with the payment card industry. The private sector regulated itself and said, “Here is what we need to have to secure credit card data,” and they forced you to do vulnerability assessments and different types of assessments. And anyone who processes credit card data applies those standards to them.

Senator PETERS. Mr. McBride, I have been a proponent of improving our understanding of geomagnetic disturbances from space weather for some time now, and I teamed up with Senator Gardner on the Space Weather Research and Forecasting Act back in 2016.

We had William Bryan, the nominee to the director of Science and Technology (S&T) at DHS a couple of weeks ago. I asked him what role his organization can play in preparing our Nation for a potential space weather event. He responded that he will work with the DHS and other customers to determine what requirements needed to be worked toward in this area.

So my question to you is, in your opinion, in what areas do we know what these requirements are, and in what areas do we need more research to better understand how our critical infrastructure may be impacted by a space weather event?

Mr. MCBRIDE. So the electromagnetic pulse threat is multifaceted. We have high-altitude nuclear detonations that create an E1, E2, E3 effect. So it is the full spectrum of the EMP pulse.

We have things like flux compression generators. We have the sun. The sun particularly—the E3 portion of the EMP pulse with geomagnetic disturbance can be minutes or even up to hours. That threat is ultimately going to potentially cause damage to large substation power transformers.

We have never combined in the models or otherwise the entire waveform associated with the EMP threat, E1, E2, and E3. I believe that is a huge knowledge gap that needs to be experimented and understood.

In addition, nobody is in charge. So DHS, we have been doing some work for the Department of Energy Office of Electricity, understanding what EMP and GMD risks to the power grid are. DHS, their mode was they asked a particular person to stay abreast of what others are doing relative to the electromagnetic pulse threat.

Department of Defense recently formed their electromagnetic defense task force, which I participated in 3 weeks ago. Nobody has really taken ahold of whose responsibility is it to mitigate this threat to the power grid.

I believe for EMP E3, with an investment of somewhat less than $4 billion, we could mitigate that vulnerability to our most key resources in our extra high-voltage power grid. That technology exists. We have tested and validated it. We know how to do it. Where we do it and who funds it is the big challenge that we face.

Senator PETERS. Thank you.

Chairman JOHNSON. As long as we just made that point, I want to talk about how reasonable that cost is. Less than $4 billion, we had testimony here earlier with Dr. Richard Garwin on the Carrington Effect that happened about 150-some years ago.

Mr. MCBRIDE. 1859.

Chairman JOHNSON. 1859.

We have generally—figure that one of those large-scale solar storms once every 100 years. Richard Garwin said we have a 10 percent chance every decade of having something like the Carrington Effect.

Again, we have been dodging that bullet now for over 150 years. If we were to experience that with today's electronics and technology, what would the cost of a massive solar storm—what would the potential cost be that we are trying to mitigate with about a $4 billion expenditure?

Mr. MCBRIDE. I believe that cost would be in the trillions of dollars, significantly less than the cost to replace the infrastructure that would fail due to a Carrington-level event.

Chairman JOHNSON. And hundreds, thousands, tens of thousands of lives lost?

Mr. MCBRIDE. Very likely. It would be the socioeconomic disaster that this country has never seen.

Chairman JOHNSON. So you take a look at Puerto Rico who lost power, but we could try and surge resources and help that. There would not be too many people coming to rescue on something like that type of event, correct?

Mr. MCBRIDE. That is correct.

Chairman JOHNSON. Again, Senator Peters, I appreciate your concern about this. We share that, and we will continue to try and figure out and get somebody put in charge of that. Senator Carper.

OPENING STATEMENT OF SENATOR CARPER

Senator CARPER. Thanks, Mr. Chairman.

We also are on multiple committees, and we just finished one of my hearings. So I am happy to be able to join you now at this hearing. I missed your testimony and had a chance to look at it, and I appreciate the chance to ask you some questions.

I am told that some of you mentioned in your testimony the Russian campaign to hack the U.S. Presidential election in 2016. Attempts by Russia and Russian government, backing actors to interfere in sovereign elections are not new. In 2014, that country orchestrated a campaign to interfere in the elections. In the Ukraine, my wife has been with some of her friends and colleagues from DuPont from years ago, has been in Georgia this week, and she is sharing with me some of what Russia tried to do in Georgia that we are familiar with.

U.S. intelligence agency or the U.S. intelligence community said in its 2016 report that a criminal will likely continue using cyber campaigns to interfere in elections for two simple reasons. They are cheap, and there seems to be no consequences.

Mr. Mandia, your testimony said much the same thing.

Yesterday, President Trump signed a general Executive Order that would impose sanctions on countries found to be interfering in our elections, but he has failed to impose sanctions on Russia, despite explicit authorization from the Congress.

The Republicans in Congress recently defeated an amendment from Senator Leahy that would have provided States with an additional $250 million for election security.

I would just ask. Again, I think, Mr. Mandia, from you and Ms. Bisceglie?

Here is the question: Do you believe the United States could do more, should do more to deter and prevent cyberattacks on our election infrastructure in order to protect our democratic processes? That is the first part of the question.

The second half of the question would be, What steps in particular do you recommend that those of us here in Congress focus on first?

Kevin, do you want to go first? Thank you.

Mr. MANDIA. Well, for the next 30 minutes, I will be outlining the steps we need to take. No, I am kidding.

But the bottom line is right now it is an interesting time to be impacting cybersecurity. Every modern nation does not know where the border is for behavior. There are no international rules of engagement, and I observed the Russian behavior from 1995 to 2000 and whatever today is.

For the most part, we have observed their offensive capability on a daily basis. I have done thousands of hours of forensics looking at some of the machines compromised from threat actors in Russia, whether criminal or government-sponsored. Sometimes it is hard to tell the difference.

The bottom line is if all we are ever doing is playing defense, we are always going to be having a little mop-up on Aisle 5 to do in cyberspace somewhere just because the asymmetry between offense and defense, it is almost hard to explain.

We are trying to defend millions of machines, but as long as there is a communication channel into your organization from another human and there is anonymity on the Internet, you are hackable. It is just that simple. Whether that communication channel is email, Skype, instant messaging. Facebook wall is just waiting for somebody and baiting them to it.

So this is a complex channel where you have to have a doctrine that imposes risk and repercussions. The problem is it is also hard to write a red line in cyberspace. The demarcation of what is acceptable and what is not acceptable is still blurry.

What I have seen in the last few years—and I am indirectly answering your question—is we are seeing indictments. We are getting attribution. We are making indictments. A lot of people ask, "Does that matter?" The answer is yes. We have a sovereign nation and a Department of Justice pointing the finger at nation-states and individuals in those nations.

Over time, even if the government cannot impose risks and repercussions, the Internet experience from nations that harbor cybercriminals and different—what I call trench warfare in cyberspace by nation-state actors, their Internet experience is actually going to be different.

There are private sector organizations that block every Internet Protocol (IP) address from Russia today. That is going to expand and expand and expand.

The bottom line is the private sector is doing what is in its realm to defend itself, and it is looking to the government to do its best to get attribution right and to impose risks and repercussions and to have some predictable doctrine so that we can govern the behaviors.

And it is going to happen. If we do not do anything soon, Senator, what we are witnessing is escalation, and the reason I told you the years I have been responding to Russia is for whatever reason, in August 2015, we saw them change rules of engagement that they followed with great discipline for the prior 20 years. Suddenly, they started targeting wider, started doing less counter-forensics, started attacking anti-Putin professors, started posting things that they stole. Those behavior changes, if unchecked, will keep escalating.

So we are going to have to sort it out. The answer to that is going to be a lot of folks sitting in the room trying to get that doctrine piece together. We have been working on this for 20 years. It is not simple. We have been admiring the complexity of it, but we have to start somewhere.

And that is enough of my statement.

Senator CARPER. All right. Thanks so much.

Jennifer, I will just use your first name, if you do not mind.

Ms. BISCEGLIE. No, that is fine.

Senator CARPER. Again, two-part question. Do you believe the United States could do more to deter and prevent cyberattacks on our election infrastructure in order to protect our democratic process? And, second, what steps in particular would you recommend that we take here in Congress? Where should we focus first?

Thanks.

Ms. BISCEGLIE. Thank you.

And I absolutely agree with everything that Kevin outlined.

Back to the Federal Information Technology Supply Team Risk Management Improvement Act, to me, this is a perfect example of where they could have some impact. It is really the players that are at that table looking at what the doctrine should be and then really looking at all of the sub-tier relationships because it is not happening at the voting machine level. It is all the components in it that expose you to a lot of the communication concerns that Kevin just outlined. To me, that is a perfect opportunity for what you have put out there to say let us really understand all the different levels, all the different players, what is important, where the opportunities are that we are exposed to, because I agree we need to have an offensive, but we do need to have a defensive at the same time because you have people involved.

And so I think if you follow the steps that Kevin just outlined, it is perfect. Take this act. Take this bill that is out there and really start focusing on the sub-tier relationships, and we are going to be better off.

The last thing I would like to talk to you—and it comes from all the questions that have been asked—you really cannot separate these two conversations. The supply chain and the cyber concern is a physical and a digital relationship, and you cannot separate those things anymore. Whether you are talking about the F–35 or logistical ports or voting machines, this is the same conversation, and it has to be done hand-in-hand or we are going to miss something.

Senator CARPER. Thanks to both of you. In fact, thanks to all of you.

Chairman JOHNSON. A quick little comment. This is really more Senate Foreign Relations Committee, but we held a hearing with North Atlantic Treaty Organization (NATO). The question I raised in that hearing last week and the one I will continue to raise is we need an attitude change. When you look at NATO, the combined economic firepower of NATO is well north of $30 trillion. Russia is less than two. How can NATO, how can the EU, how can America allow that puny little economic power push us around this way? Because we just have to change that attitude. We are the 800-pound gorilla, and it is really absurd what we are allowing Russia to get away with.

But, anyway, I have questions. I want to ask each of you—and I will start with Mr. McBride. Who should be in charge of this effort? Which Department, which agency is best positioned to be in charge of GMD, EMP, and I would say even responsible for reestablishing the grid, even with a cyberattack?

Mr. MCBRIDE. I believe as the sector-specific agency for the electric grid in the United States, the Department of Energy should be in charge of mitigating this threat.

Chairman JOHNSON. So, obviously, Department of Defense, Department of Homeland Security would be involved in that, but the lead agency should really be the Department of Energy?

Mr. MCBRIDE. I believe that to be the truth. Yes.

Chairman JOHNSON. OK. Ms. Lanier, when it comes to drones, what do you think? You have been in law enforcement. Who should be in charge of that effort?

Ms. LANIER. Well, in charge of the effort, I would say probably DHS.

Chairman JOHNSON. Because right now, it is FAA.

Ms. LANIER. Correct. I would say probably DHS.

And I would also say that, as I mentioned in my testimony, both my written and my oral testimony, I think it is really important that we find some way to integrate State and local law enforcement on the back side of that DOJ–DHS effort. I think they are really important. That is why they are the first responders.

And the threat that is posed by drones that detect and interdict, it is going to be critical to have State and local law enforcements tied in there.

Chairman JOHNSON. Mr. Mandia and Jennifer, in terms of cybersecurity, who should be taking charge?

Mr. MANDIA. It is going to depend on mission. It is that simple.

Right now, when it is law enforcement, you see the FBI primarily present, but local law enforcement will be present as well.

In regards to other operations in cyber, you will have the intelligence agencies. I just think it is more complex because you also had the private sector, and there is usually an alignment by industry where energy companies and utilities are aligned to figure out what is best practice for us and what do we do. The financial services and the Financial Services Information Sharing and Analysis Center (FS–ISAC) are aligned. So you see the private sector trying to regulate the private sector in many ways as well. I gave you that example, the payment card industry.

I think it is hard to pick. Do you have one cyber czar in charge of all this when you have so many missions and so many industries impacted by it?

Right now the system is working pretty well. I think probably the biggest change we could make in the government is because there is a shortage of cybersecurity professionals, you may want to have the DOD doing what they do. The intelligence agencies are doing what they do, and there may be other agencies like FAA and a few others that need to do it alone, but there is probably an opportunity to consolidate a single computer emergency response team—that is the security operations center for 100 government agencies. Why not? We do not have the effort to do it.

Chairman JOHNSON. Where should that be housed?

Mr. MANDIA. Sir, I would pose that question to you.

Chairman JOHNSON. Well, Ms. Bisceglie.

Ms. BISCEGLIE. So it may be a little snarky, but my point is whoever is going to actually do it is who should do it.

Chairman JOHNSON. That would be good criteria, right.

Ms. BISCEGLIE. So the latest one I have seen for supply chain in cyber is Homeland Security. If we are going to do this—and I do agree with what Kevin, again, just laid out.

But my thought is I would have a dotted line. I would have the alignment by industry because even when you look at an industry, you have all the different pieces that go into it. So I would have the dotted line to Department of Energy, to the DOD, to whatever they are responsible for, get away from the partnerships. The idea of a GSA and DHS partnership is really very difficult. Somebody has to be responsible.

And then, again, get away from the political agenda, which to the point that you just said forces that cultural shift that really needs to occur.

Chairman JOHNSON. You have all mentioned that you really need the information sharing with private sector and government. That has always been the problem with DOD taking charge, and that is one of the reasons people look at DHS as kind of the default agency that can work with private sector.

But, again, who has the greater capability?

Ms. BISCEGLIE. So, in my opinion—and I do not want to put myself out of business, but this is—to the point that you said, this is a culture.

There was actually a memo that you are probably aware of that went around last year in the Department of Defense that actually gave their people permission to talk to industry. That is not a law. That is a culture. And so the more that we help folks understand that businesses are the ones that are going to solve this—this is not government to solve. Regulatory, I agree with. It is businesses to solve and change the culture.

Chairman JOHNSON. I think there may be reluctance from the private sector to be contacting DOD or NSA.

Mr. McBride, I will just have you chime in on this one on cyber. You have some knowledge of this.

Mr. MCBRIDE. Yes. So, for several years, Idaho operated the Industrial Control Systems Cyber Emergency Response Teams (ICS–CERT). So we were in a reactive mode. Where there is an attack in the Ukraine, we send fly away teams out, collect that forensic data from their networks. We reverse-engineer that in our malware lab, understand what the malware can do, and develop mitigations for that.

Department of Homeland Security has now closed the ICS–CERT, and now it is all operated through the National Crime Information Center (NCIC) here in—I believe DC.

Sharing information with the asset owners that need to know what the threat and intelligence is has been a difficult problem. I think we can improve that. Some people are now getting security clearances, where the threat intelligence can be shared with them.

There is a new program that has just been stood up that is trying to change from a reactive mode into more proactive. Countries like Chechnya, Estonia, the Ukraine, they have told us that they feel like they are test beds for Russia. So Russia develops a cyber capability. They exercise that on one of these three countries.

We have people all over the world collecting intelligence. We want to be able to develop mitigations for threats, vulnerabilities, and malwares that are discovered prior to arriving on U.S. soil.

The intent is to create a proactive mitigation strategy for cyber threats.

Chairman JOHNSON. OK. But do you all agree somebody has to be in charge? I mean, this cannot be five, six, seven different agencies, just line authority and nobody really with the authority to make sure that there is commonality in our approach and that type of thing. Just yes, yes, yes, or what is it?

Mr. MANDIA. It is tough because I still think it aligns by industries. If there was an all-out cyber campaign against this Nation, you are going to see the financial services circle the wagons. You are going to see the utility circle the wagons. Largely, a lot of the attacks against those two groups may be wholly different.

If you are attacking a utility to shut it down, the attack looks one way. If you are attacking the financial services to disrupt it, it may look a little bit different.

What I have observed in threat actors is they actually do align a little bit by industry. So you will circle the wagons that way.

Overall, coordinating that event and that response, it is hard from where I sit to say it is not the DOD during times of war.

With that being said, during times of perceived peace, right now, I have observed we have a shortage of folks to protect our networks. It would make sense to centralize for most government agencies that defense component and capability.

Chairman JOHNSON. I am just going to continue down my list. I have a lot of questions here.

Mr. Mandia, you are talking about attribution——

Senator CARPER. Mr. Chairman?

Chairman JOHNSON. Pardon?

Senator CARPER. Could I just follow up on your question?

Chairman JOHNSON. Sure.

Senator CARPER. It is just a follow-on, if I can.

When we passed out of this Committee legislation reauthorizing DHS, one of the provisions in that reauthorization dealt with National Protection Program Directorate (NPPD) and in which we sought to make it clear that they had the skills, the responsibility and so forth to work in this arena.

I think a bunch of us believe that we all share the goal of ensuring that NPPD functions as a full component of the Department and it has resources that are necessary to carry out what we all think is a critical cybersecurity mission.

Would any of you care to comment on the importance of authorizing a dedicated cybersecurity agency within DHS to work with the private sector in order to address these kinds of threats?

Ms. BISCEGLIE. I think it is very important. I think it is important to have somebody in charge with a charter, and if NPPD is the place, they have to have a charter. They have to be resourced appropriately from a skills set standpoint as well as financially, and then they need to be held accountable and again not just around activity but for the integration across the players, as Kevin keeps outlining, and what are we actually doing about it?

Senator CARPER. Thank you.

Anyone else?

Mr. MANDIA. Centralized is going to be better than decentralized.

At the end of the day, you look at what Britain did and the UK. They have one place where everybody reports every single event to, not a multitude of them. Overall, you will have a better learning system if you do centralize all the intel coming in and have one coordinating point. Yes.

Senator CARPER. All right. Thank you, Mr. Chairman.

Chairman JOHNSON. Israeli has one directorate reporting right to the prime ministers. So we need to look at those models.

But, Mr. Mandia, you were talking about attribution offense. What came to my mind during that process was just definition of the problem too.

I have been doing this for 7 years, and I kind of define the whole cyber issue in four buckets—crime, cybercrime; espionage, industrial espionage; then just malicious activists, OK; and then warfare, those four buckets.

I completely agree with you. As long as we are just on defense, that is where we are going to be, and offense is going to get better and better capabilities.

You need to have some kind of deterrent, but the problem there is attribution and if you go on offense, to do it right. Can you just speak to that concern?

Mr. MANDIA. Well, I do know this. You can easily frame it exactly how you just did. You have criminals. You have espionage. You have just malicious intent, destroy whatever you can, and you have warfare.

But what we observed was amazing for me. In September 2015, we had some kind of agreement with China. I do not know if it was written or not, but what we observed in cyberspace is prior to August 2015, we saw between 60 to 80 U.S. companies compromised every month from cyber espionage campaigns out of China. August, it goes down to four.

Chairman JOHNSON. And you wrote the book on that, right?

Mr. MANDIA. Right. Well, we exposed it in New York Times in 2013 just because it felt unfair having folks barge into a building in a military unit and hack into a brick-and-mortar firm in the United States, did not seem like a fair fight.

The bottom line is we saw, after some agreement was reached, those attacks go down to four and hold steady for a long time. So there are certain nations we can, in fact, have agreements on rules of engagement, and I would argue, we have had them for decades with Russia even until recently. It seems like they have escalated.

So where you can get that kind of agreement, we should do it, and where you cannot, that is where the complexities arise.

Chairman JOHNSON. Well, to get back to your point about too much classification—again, I will go back to Kaspersky. When we first found out about that, we knew about them for almost a decade. We allowed that business to grow and be a security platform for most computers here and exposed ourselves. To me, that public exposure is incredibly important.

I mean, in your Mandiant report, I think it was 2014 on the People's Liberation Army (PLAs) little operation there.

China, I think is particularly sensitive to public exposure and disclosure on these things.

I think Russia certainly could possibly, as long as we are making them pay a price for these things.

I could not agree with you more that we way overclassify these, and it is to our own detriment. And we are saying we do it for national security, and I think we are actually risking our national security by not making more of these things public.

I want to talk a little bit about government control versus private sector. Private sector would be more nimble. When I sat in a hearing over there early on—this was in probably 2012—talking about the Collins-Lieberman bill, a representative from DHS—I asked him point blank, "How long will it take you to write the regulations, contemplating this piece of legislation?" With a straight face, he said about 7 years.

To me, an insurance model will really help discipline this process. I would like you to talk a little bit about that, Mr. Mandia, because you sort of touched on this. Where are we in terms of ensuring cyber risks, and do you think that is an effective model?

Mr. MANDIA. Well, I do think it has been in the discussion since the late 90s. When you look at risk, most CEOs want to deploy their own risk framework to their organization. If you are not a regulated entity, it is your risk profile that you need to implement at your company.

I do believe insurance—I think it is inevitable, quite frankly. We have talked about it for multiple decades, but there is cyber insurance available, and the question becomes who sets the floor for how good we are at cybersecurity?

It is real hard for the government to have sweeping legislation that says here is how good you need to be whether you make cupcakes, make hamburgers, or make missiles.

I do not think it works. I think you can self-regulate, and the private sector can do this. And insurance is probably one way where that can come to fruition. That if you do want cyber assurance and maybe even you have to get it if your company is shaped a certain way, has a certain number of employees, or for maybe certain industries. We have regulations for utilities. We have them for financial services. Those are pretty much taken care of, but for a lot of the mom-and-pop shops that are driving business, maybe insurance is the right route in that they get—basically it will be the insurance companies that say here is how good your cybersecurity needs to be, here is the floor, and at least we can start benchmarking the infrastructure security.

Chairman JOHNSON. Well, then through the supply chain too, like International Organization for Standardization (ISO) certification, you can also certify sub-tier suppliers to do those audits again. That can all occur in the private sector.

Senator McCaskill, do you have any further questions?

Senator MCCASKILL. No.

Chairman JOHNSON. Let me in this case—because, again, we had some good questions. We have some real experts here. Is there something that somebody touched on that we were not able to really kind of flesh out?

I will just kind of go down the list or down the witness panel here. Is there something you want to say just in a closing comment? Mr. Mandia.

Mr. MANDIA. No. I have said enough.

Chairman JOHNSON. OK. Ms. Lanier.

Ms. LANIER. Yes. I think I missed an opportunity to reemphasize the main points that we wanted to get across today.

Again, I mentioned in my written testimony, we support the Federal Aviation Administration's efforts to adopt and implement the remote identification requirements for all or nearly all drones that are sold or operating in the United States.

We also feel that Congress should revise the hobbyist exemption in Section 336 of the FAA Modernization and Reform Act of 2012. The current hobbyist exemption permits far too many drones to be operated by unlicensed and untrained pilots.

And we support the aims of your bill. The Preventing Emerging Threats Act of 2018, which would extend drone interdiction authority to Department of Homeland Security and Department of Justice. The bill represents an important step forward in helping to provide greater protections. We just want it to go a little further and include State and local law enforcement officers that are on the front lines every day at mass gatherings trying to protect thousands of people.

So thank you for letting us participate.

Chairman JOHNSON. That would be next step, no doubt about it. Mr. McBride.

Mr. MCBRIDE. So I would like to mention that in the United States, we have public power utilities like Request for Equitable Adjustment (REAs), co-ops, and municipals. They are owned by their members, by their customers, and they are unregulated. And then we have the investor-owned utilities which are regulated. They are regulated by the State public utility commissions and by the Federal Energy Regulatory Commission (FERC). I think it is important that government-private partnership be developed because the utilities that are not regulated, unless they are told they have to do something, they are probably not likely to do it. So I believe the responsibility to the asset owners would be to identify, do the modeling and analysis, to identify those critical assets that need the protection against the threat of EMP or GMD, and then the government, I think has to help them implement the mitigations for those.

Chairman JOHNSON. Thank you.

Ms. Bisceglie, did I ever get that right?

Ms. BISCEGLIE. That was awesome. You did.

Chairman JOHNSON. Oh, OK. Great.

Ms. BISCEGLIE. I think our biggest thing was to really centralize it and line item fund it, but on your last question, if I could, the difference to government and the private sector, I think the biggest thing—and again, I think that the bill for the Federal Information Technology Supply Team Risk Management Improvement Act, the Government really needs to understand what they are inherently responsible for and what is important to them. So is it the voting machines that were involved in the Census 2020? What is important? Use this act to actually drive that home.

Focus on that risk tolerance. That is where the regulations, the policies, the auditing that was just mentioned by Mr. McBride—we do not get asked. Like Continuous Diagnostics and Mitigation (CDM), the latest version of CDM actually has a supply chain risk management as a requirement in procurement, and nobody is being audited against what is being done or not being done. I think it is a great question to ask.

And then I think the last thing is what I mentioned before. Again, I did hear a lot here. In any of these things, we cannot separate cyber and supply chain because they are one-in-one, hand-in-hand right now.

Thank you.

Chairman JOHNSON. Again, thank you.

I cannot help but notice and comment on the fact that prior to this hearing—this was always Senator McCain, who—again, we all respected—in his last couple of years as Chairman of Armed Services, he was not in this Committee as often, but we all traveled with him. We saw his commitment to individual liberty, freedom, the type of hero he was not only in America, but you go over to Ukraine because he was fighting for, again, those kind of democratic values.

So we already do miss him. We sorely miss him. I am reminded just kind of looking at a different name in his spot.

And I also want to welcome Senator Jon Kyl, who I also have a great deal of respect for. He has done a lot of work in terms of national security, maintenance of our nuclear stockpile to keep this Nation safe.

So I wanted to make those comments as we close out this hearing.

But, again, thank you for your testimony. You put a lot of work into it. You really did. I appreciate that. They will be in the record, and the hearing record will remain open for 15 days until September 28, 5 p.m., for the submission of statements and questions for the record.

This hearing is adjourned.

[Whereupon, at 12:04 p.m., the Committee was adjourned.]

APPENDIX

Chairman Johnson's Opening Statement
"Evolving Threats to the Homeland"
Thursday, September 13, 2018

As prepared for delivery:

The purpose of this hearing is to increase the public's awareness of evolving threats to the homeland, specifically cyberattacks on critical infrastructure, unmanned aerial systems, electromagnetic pulses and geomagnetic disturbances, and risk to our communication and information technology supply chain. Any of these threats could cause significant damage to the nation and the lives of everyday Americans.

Cyber attacks against critical infrastructure, commercial and military assets represent a growing threat to our national and economic security. This issue is complex, and promises to become even more complex as technology progresses. We need to properly define the problem and organize our efforts to counter what could create an existential threat to our nation.

Unmanned aerial systems, or drones, could pose a variety of threats to the United States. To address this threat, the Committee passed the Preventing Emerging Threats Act of 2018. The bill would provide the Department of Homeland Security and the Department of Justice necessary authorities in an attempt to counter malign use of drones. We know the threat is real. In 2011, the Federal Bureau of Investigation arrested and charged a U.S. citizen for planning an attack on the Pentagon and U.S. Capitol with an explosive attached to a drone. Just last month we saw news reports of explosives-laden drones used to target the Venezuelan dictator Nicolas Maduro. I urge Congress to swiftly pass this important piece of legislation so we can address this threat.

Electromagnetic pulses and geomagnetic disturbances are low probability, but high-risk occurrences that possess the ability to cause significant damage to our nation's critical infrastructure. To date, federal progress to address this risk has been woefully inadequate. The Department of Homeland Security has not finalized a strategy to protect and prepare U.S. critical infrastructure against electromagnetic pulses and geomagnetic disturbances, as required by a provision included in the 2017 National Defense Authorization Act. I am concerned that the Department is not making enough progress to address this vulnerability.

Finally, communication and information technology supply chain threats are increasingly pervasive and dangerous. The National Counterintelligence and Security Center has described our country as being "under systemic assault by foreign intelligence entities" who use our supply chains as vectors to commit espionage and steal valuable trade secrets. The risks posed by these threats have the ability to undermine our democracy, diminish our national security, and weaken our economy.

Today's hearing will solicit opinions from experts on how the federal government is addressing these evolving threats. I want to thank the witnesses for being here today, and I look forward to your testimony.

supply chains within our government agencies and the U.S. infrastructure. This evolving threat can turn a mundane anti-virus software purchase into an unacceptable risk to our national security. We need to make sure our information technology products and services are safe from infiltration - down to the smallest component, and like most national security issues, that requires a strategy and a whole-of-government approach.

Supply chain risk management cannot be achieved piecemeal. In this regard, a threat to one agency is likely a threat to many others. In June, Senator Lankford and I introduced The Federal Acquisition Supply Chain Security Act to address this critical issue. Few understand this issue better than some of the experts on this panel. I hope this hearing will provide the Committee, federal agencies, and the public with a better understanding of the problem and how to solve it.

Similarly, this Committee has heard from numerous cabinet officials and experts in the public and private sectors about threats posed by drones. Chairman Johnson and I introduced legislation that would authorize the Department of Homeland Security and Department of Justice to conduct limited counter-drone operations, for a narrow set of important and prioritized missions. Our bill is just the first step in tackling this mounting problem, and we welcome additional thoughts from the witnesses on solutions to mitigate the threat.

U.S. Senate Committee on Homeland Security and Governmental Affairs
"Evolving Threats to the Homeland"

September 13, 2018

Ranking Member Claire McCaskill

<u>Opening Statement</u>

Thank you, Mr. Chairman. Two days ago marked the 17th anniversary of the September 11 attacks on this nation. It's a somber reminder of the threats we face and that we must continue to vigilantly protect the country from those who wish to do us harm. In the 17 years since 9/11, Congress and the American people have had spirited debates surrounding the nature of threats to the United States and how best to protect ourselves from them. A lot has changed over these nearly two decades, but until recently, one component remained constant.

Since joining the Senate over 30 years ago, my friend and colleague, Senator John McCain, was an integral part of every national security conversation that took place in this body. His commitment to public service, his dedication to the defense of our country, and his efforts to promote American values were unparalleled. I had the privilege of serving with him on this committee and on the Armed Services Committee. His conviction, insight, and sense of humor will be sorely missed. John McCain made an indelible mark on the security of this nation and I will miss him as a colleague and partner in addressing these complicated issues. I also welcome Senator Kyl back to the Senate and to this Committee, and I look forward to working with him.

The United States has made enormous progress in preventing another 9/11-style attack, but threats to the country remain. Terrorism continues to evolve as a threat and requires innovative solutions to confront and prevent it. As the United States and the world become more digitally connected and as technology advances at a rapid pace, new vulnerabilities threaten our security. This hearing provides an opportunity for the Committee to focus on some of those concerns and explore solutions to emerging problems.

In 2013, for the first time, then-Director of National Intelligence James Clapper prioritized cyber threats above terrorism when testifying before Congress. In the years since, the problem has metastasized. The threat of cyberattacks and cyber espionage regularly dominate headlines, and with the midterms approaching, election security is of paramount concern. This Congress, Senator McCain, as chairman of the Armed Services Committee, created a cybersecurity subcommittee on which I serve, where our focus compliments the work of this Committee on identifying cyber threats and strengthening our forces and capabilities.

One area of focus that I am particularly concerned about is supply chain risk management and specifically, the information technology and telecommunications

I want to thank the Chairman for holding this hearing and look forward to the discussion.

PREPARED STATEMENT OF KEVIN MANDIA, CEO, FIREEYE, INC.,

SENATE HOMELAND SECURITY & GOVERNMENTAL AFFAIRS COMMITTEE

Evolving Threats to the Homeland

SEPTEMBER 13, 2018

Mr. Chairman, Ranking Member McCaskill, and members of the Committee, thank you for the opportunity to share FireEye's perspective regarding cyber threats to the United States of America.

Before I begin discussing cyber threats, I would like to take a moment to extend our condolences to each of you for the loss of your dear friend and colleague, Senator John McCain. His distinguished service in the U.S. Navy and in Congress was an inspiration to us all. He represented Americans, and he represented the best of American values.

My testimony today is derived from FireEye's unique visibility and experience responding to significant breaches around the globe, from the intelligence collected and produced by our cyber threat analysts, and from the products our customers use to detect intrusions and respond to attacks. I intend to discuss the cyber threats to our nation, what their impact could be, and some of the major actions we could take to prepare for these threats.

Introduction

I have been working in cybersecurity for more than 20 years, since I was first stationed at the Pentagon as a Computer Security Officer for the United States Air Force, and later as a Special Agent in the Air Force Office of Special Investigations, investigating computer intrusions into our military networks. My entire career has been dedicated to cyber security, and I have had the honor of serving as FireEye's CEO since 2016.

FireEye is on the front lines of the cyber conflict every day. We have over 100 threat analysts, in 18 different countries, covering 32 different languages, tracking cyber attackers. We have over 300 security experts, working in 26 countries, investigating successful network intrusions. We review over 1 million new malware samples everyday, and we have over 15 thousand global sensors - detecting anywhere from 50 thousand to 70 thousand malicious events per hour.

Today, through a shared services contract with DHS, more than 100 departments and agencies are using FireEye Threat Intelligence in their security operations. We collect, prepare, and disseminate intelligence on cyber threats daily, and the discussion I can share today is only a fraction of the intelligence we have accumulated.

The Threats to the United States

Let me begin by sharing three general observations about cyber threats to the United States.

First, I believe the United States is uniquely more vulnerable in cyberspace than other nations. We are a lot more dependent on the Internet, technology and network infrastructure than the nations that host the most prevalent cyber attackers. Second, much of our critical infrastructure is privately rather than publicly owned, requiring more private/public partnership to defend our infrastructure. Finally, our freedom of the press – a foundational ingredient of our democracy – allows adversaries to achieve two types of attacks that are far less impactful in closed societies – the ability to conduct influence operations on the American public – and the ability to release or threaten the release of private information stolen in the latest data breach as leverage to elicit some behavior.

Second, while public discussion about cyber attacks frequently focuses on "Cyber Pearl Harbor" scenarios, I believe that our nation is more likely to face an enduring, more protracted cyber campaign akin to "cyber trench-warfare."

1 – The first characteristic of cyber trench warfare is that it will likely be conducted below the threshold of actions that might elicit a formal, aggressive response by the United States.

2 – Second, these campaigns will be long-term, resource-draining cyber operations.

3 – Third, they will target the whole-of-society rather than just military and government networks, seeking to wear down our morale, trust, and readiness without resorting to a single, game-changing attack. Looking back on my experiences in both the military and in the private sector, it is clear to me that our nation's greatest vulnerabilities are not the defense and military networks or the large critical infrastructure providers. Instead it is the targeting of everyday Americans and their businesses. These softer targets, such as individuals, state and local governments, public schools, academia, smaller businesses, form the fabric of our daily lives. Not every company or organization has the resources or capabilities to defend itself in cyberspace, and a catastrophic or even gradual failure of the softer targets will result in significant impact perhaps as grave as attacks against well protected, critical systems.

4 – And lastly, Cyber trench warfare will have a persistent negative economic impact.

Based on these qualities, there are some security experts who would opine that we are already engaged in "cyber-trench warfare" today.

My last general observation is that any of the damage from cyber conflict easily spreads to impact many facets of our daily lives – and the impact will continue to grow as we live more connected. We refer to this widening impact as the "butterfly effect." The most poorly defended businesses might be the ones most targeted, and certainly the one's most impacted during a cyber conflict, and the impact would permeate our daily activities in ways that can be difficult to predict.

Now I would like to discuss some specific threats to our nation that we ought to prepare for.

The Threat to Utilities

American utilities will likely be targeted during any future armed conflict and would also be prized targets to groups or lone actors with malign intent.

At FireEye, we have seen the targeting of critical infrastructure in the Middle East, where adversaries disrupted the safety systems of a utility provider. In Ukraine, we observed attacks on the electrical grid, disrupting businesses and homes across the country. We alerted the public to North Korean spear-phishing attacks of U.S. electric companies late last year, as threat actors attempted to manipulate workers into clicking on illicit emails.

While most large-scale utility companies have complex redundancies to protect against large-scale disruption, smaller utility providers may be less-equipped to defend against nation-state level cyber activity. It has been our opinion, while the bigger, well-resourced utilities may operate through an advanced cyber attack, the less resourced, more rural utilities are at a higher risk of failure. Therefore, the probable impact of a sophisticated, prolonged cyber attack against American utilities will have far more negative impact on the vital services in rural areas and smaller municipalities than in the major cities.

The Threat of Indiscriminate Attacks

The United States can expect future attacks that are indiscriminate, seeking to effect as many citizens as possible at once. These attacks would be intended to disrupt business as well as personal endeavors and would have wide-ranging impact.

For example, North Korean actors used ransomware to conducted anonymous mass extortion to obtain crypto currency. Other nations will likely adopt this tactic for political ends. Attacks like these can also be financially destructive; June 2017's NotPetya ransomware attack caused approximately $10 billion worth of damage, according to government estimates.

As a hypothetical, one can imagine a nation wanting to compel a response of some kind from another nation. Instead of using military force or economic sanctions, it could choose to release ransomware targeting that country's citizens, critical infrastructure, and government functions – not returning the use of encrypted data being held for ransom until the desired response is taken. With the anonymity of the Internet, nations could spread doubt by claiming such an attack was the work of cyber criminals and hold entire nations hostage with limited risk or repercussions. This scenario is notional, but ransomware's capability to have widespread impact and its reversibility make it likely to be deployed in the coming years for strategic gains.

The Threat of Information Operations

We have heard about Russian Information Operations, but the number of nations leveraging social platforms and incorporate today's technologies are expanding. Just two weeks ago FireEye announced the discovery of an Iranian influence campaign extending from the Middle East to Europe and the Americas.

Information operations are likely to be a persistent force in media and society from now on. The evolution of information operations allows Nations to individualize their efforts, and to be informed person-by-person by our likes, shares, and other information freely available on social media.

Artificial intelligence will add to the effectiveness of these information operations. Nations will be able to draw on massive data sources of information to curate content tailored to the characteristics of each user. AI is also giving rise to entirely new threats, such as deep fakes— or counterfeit content so realistic that we may soon no longer be able to trust that a video we see, or a sound bite we hear, is authentic.

What the U.S. Can Do to Prepare for These Threats

There are many actions the United States Government and the private sector can do to help mitigate the impact of these threats, and today I would like to mention a few of these actions. We should accelerate a coordinated defense against the cyber threats to our nation by promoting a system that fosters actionable and timely information sharing, supports the practice of resiliency in businesses, secures the supply chain, and identifies and holds perpetrators of cyber-crime or cyber trench-warfare accountable.

Information Sharing

The sharing of actionable threat information will narrow the security gap facing businesses and organizations today. Government, including law enforcement, and some companies have this actionable intelligence. We need to create a way in which they can share this information in a standard, codified, machine-readable way that does not betray or diminish the effectiveness of our national security or law enforcement missions, or significantly impact our privacy and civil rights. If we do it right, sharing threat information will promote an aggressive, dynamic "learning system" of cyber-security for the nation. Effective information sharing:

1 – Acts as an early warning system giving potential victims advance notice of significant threats;
2 – Promotes technologies that facilitate the effective use of threat information;
3 – Empowers the private sector to defend itself more effectively; and
4 – Significantly reduces the duration and impact of breaches, should they occur.

The private sector cannot do this alone. Our nation must find ways to unite the American people and their businesses in a common defense alongside federal, state, and local network defense missions and to combine efforts with our allies in Europe, Asia, and the Middle East.

Promote Resiliency

As a country we also need to start thinking more about cyber resilience. Can major commercial enterprises continue to function if some or all of their internet-connected systems are disabled? Can the military deploy and command troops? What about the civilian government?

Few companies can adequately predict all the business operations or processes that are impacted by loss of Internet connectivity. I urge the Committee to consider ways it could require government agencies to develop and carry out continuity-of-operations plans that practice, even for just 24 hours, going without Internet connectivity while continuing critical functions. Private sector companies, too, would benefit from this model.

Strengthen Supply Chain Resilience

Threat actors have increasingly leveraged the trust between users and software providers. Users do not expect malicious code to be introduced by updates from trusted software vendors. In supply chain attacks, cyber threat groups target the build servers, update servers and other parts of the development or release environment. The hackers then inject malware into software releases, infecting users through official software distribution channels. This method allows attackers to target broad set of potential victims while obfuscating their intended targets.

In 2017, FireEye observed at least five cases where advanced threat actors compromised software companies to target users of the software. Chinese cyber espionage operators modified the software packages of a legitimate vendor, NetSarang Computer, allowing access to a broad range of industries and institutions that include financial services, transportation, telecommunications, energy, media, academic, retail, and gaming. Likewise, in June 2017, the NotPetya ransomware was spread to various European targets when Russian actors compromised Ukrainian software vendor M.E.Doc. I am confident that advanced attackers will continue to leverage the software supply chain to conduct cyber espionage.

Hold the Perpetrators Accountable

Every day there is an onslaught of cyber attacks impacting American business and individuals. The largest contributor to the rising occurrence of these cyber attacks is that there are no risks or repercussions for those who commit them. Adversaries now believe they can attack our economy, our way of life, and our continuity of government without provoking a military response, so long as they do so in cyberspace. In short, there is no deterrence. Until we as a nation hold these threat actors accountable, we will likely continue to get sucker-punched in cyberspace.

Policymakers should continue diplomatic efforts to proactively define the rules of engagement with our international counterparts so that they expect a clear, consistent US response to each and every cyber attack. The agreement President Obama reached with President Xi in September 2015 to end cybertheft of commercial intellectual property between the U.S. and China led to significant decrease in operations stealing American intellectual property over the last few years. The effect this agreement had bringing adversary behavior in line with clear rules of engagement shows diplomacy can be an effective and enforceable means of peacefully improving America's cybersecurity.

Conclusion

The threats to our nation and to the world are growing, and we must be prepared to counter them. By establishing a system where the private and public sectors work together, practice together, and proactively use threat intelligence, America will build a dynamic cyber-defense system that grows smarter and more capable by the day. By exploring international rules of engagement and holding threat actors and the Nation's that harbor them accountable for their actions, the United States, and the daily lives of our citizens, will be safeguarded from the protracted cyber campaigns we are withstanding today.

Thank you very much, Mr. Chairman.

Cathy L. Lanier
Senior Vice President of Security
National Football League

Evolving Threats to the Homeland
Committee on Homeland Security and Governmental Affairs
United States Senate

September 13, 2018

Chairman Johnson, Senator McCaskill, and Members of the Committee, thank you for the opportunity to testify today on emerging and evolving threats to homeland security. As the Committee requested, I will focus my testimony today on the significant and rising threat posed by the malicious use of unmanned aerial vehicles, or drones, to large gatherings of people, including major sporting events.

As you may know, I joined the National Football League in September 2016 after more than 26 years in local law enforcement in the District of Columbia. At the NFL, I oversee the security policies and procedures that protect the 1,700 professional players, the hundreds of coaches and other staff associated with our 32 clubs, and the 17 million fans who attend our games each year. Club security officials and I work closely with local law enforcement officials, federal authorities, stadium owners, and many others to provide a safe and secure environment for our fans to enjoy the games. In addition, I serve on the Homeland Security Advisory Council, participate in the Department of Homeland Security's Critical Infrastructure Partnership Advisory Council Working Groups, and have a leading role related to security efforts and recommendations for large-scale sporting events.

In the two years that I have been at the NFL, we have observed a dramatic increase in the number of threats, incidents, and incursions by drones. Fewer than ten miles from here, a drone flew over FedEx Field during pregame activities for Monday Night Football in 2014. That operation violated the national security airspace around Washington, D.C., in addition to violating the airspace restriction over NFL games. In 2018, the NFL recorded about a dozen intrusions by drones at stadiums during games. And the NFL is not alone. In May 2017, a drone flew through Petco Park in San Diego and then crashed during the seventh inning of a game between the San Diego Padres and Arizona Diamondbacks.

An incident involving two NFL stadiums on November 26, 2017, dramatically demonstrates the threat. On that day, I received a call from the stadium security director at Levi Stadium, alerting me that a drone had just dropped leaflets over the seating bowl near one of the end zones. The NFL's game day operations center alerted other stadiums, including the nearby Oakland Raiders, which also had a game the same day. When the operator sought to fly the drone over the Oakland Coliseum, local law enforcement was ready for him. They quickly identified the operator and arrested him. The subsequent investigation revealed that the operator had undertaken extensive efforts and planning in advance of the incident. The operator had customized the drone for dropping leaflets, and he had conducted test flights to refine the drone's operations.

We are all very fortunate that the drone over Levi's Stadium dropped only leaflets. Drones today are capable of inflicting much greater damage. In 2015, the Federal Aviation Administration and Connecticut police investigated a drone equipped with a handgun. In 2017, ISIS reportedly used drones armed with grenades against Iraqi armed forces. Last year, Mexican authorities seized a drone equipped with a significant amount of explosives and a remote detonator.

As the Committee knows, various threat assessments conducted by the U.S. government and others have recognized that large gatherings of people are enticing targets for malicious actors. Consistent with those assessments, the Federal Aviation Administration and Congress have imposed restrictions on the airspace above large sporting events.

Following the terrorist attacks of September 11, 2001, the Federal Aviation Administration established flight restrictions over stadiums and other large gatherings. Congress subsequently strengthened and codified these requirements. The current version of the temporary flight restriction prohibits all aircraft operations over certain sporting events for one hour before until one hour after the event, from ground level to 3,000 feet, and within a radius of three nautical miles. In addition to NFL games, this flight restriction applies to Major League Baseball games, NCAA Division One football games, and NASCAR Sprint Cup, Indy Car, and Champ Series races. The flight restrictions designate the airspace as National Defense Airspace, and any operator who knowing or willfully violates the flight restriction may be subject to criminal penalties.

The temporary flight restrictions above stadiums and other sporting events apply broadly to all aircraft operations, including both general aviation and commercial aircraft, and flights under both visual flight rules and instrument flight rules. Importantly, the flight restrictions apply to all aircraft, whether manned or unmanned. The Federal Aviation Administration has worked extensively to educate the aviation community about the flight restrictions. Air traffic control personnel and licensed pilots have worked cooperatively to respect this protected airspace. As a result, the temporary flight restrictions over sports events have largely worked as intended, keeping commercial and civil aircraft away from stadiums during games.

Unfortunately, in my experience, drones present an entirely different challenge. Unlike traditional aircraft, unregulated drones can be acquired easily and cheaply by anyone, anywhere, anytime. Highly sophisticated drones are widely available at retail stores and online. Drones are sold to the general population for use by unlicensed individuals, often with no awareness of airspace rules, flight restrictions, or many other regulatory requirements related to aircraft. Drones are sold broadly without regard to applicable flight restrictions. For example, although drone flights are prohibited throughout Washington, D.C., numerous electronics stores and other retailers market drones in the city without notifying customers that a local flight would break the law. Unlike licensed pilots who must undergo specific training and are required to check for flight restrictions before each flight, many drone operators are untrained and simply unaware of the flight restrictions that apply to stadiums.

In our experience, the vast majority of game-day drone incursions are caused by hobbyists seeking to obtain a unique picture or video, perhaps to post on social media. Some of these operators know that their actions are unlawful, but others do not. Even if the operator is not set on causing harm, drone operations at stadiums present significant risks. For example, the Federal Aviation Administration generally prohibits drone operations over people because a wayward or malfunctioning drone can cause serious bodily injury if it crashes into a crowd. Drones can also cause confusion for fans who do not know whether a drone is a threat or part of the program. Ironically, after the incident at the 49ers game last November, some fans reported that they thought the drone was dropping free merchandise and they rushed toward it.

Stopping unauthorized drone flights at stadiums is extremely challenging. Drones are small and easily portable. Unlike manned aircraft, drones can be launched quickly and in close proximity to a stadium, such as from a stadium parking lot. The Federal Aviation Administration established the three-mile radius of the stadium flight restriction to allow authorities to have some warning about an aircraft that was purposefully violating the airspace, hopefully before the aircraft was in a position to threaten the stadium and fans.

Several stadium security directors have told me that they are regularly approached by vendors selling drone countermeasure equipment. The vendors acknowledge, and the security directors readily know, that using such devices is illegal. The current state of the law, however, leaves security officials with an unenviable choice: Procure equipment whose use would be illegal, or remain unequipped to respond to a security threat that could endanger tens of thousands of people.

To help the clubs in this difficult environment, the NFL has developed and published best practices and standards for responding to drone incidents. These best practices, which are incorporated into our overall best practices for stadium security, include suggested procedures for notifying local and federal authorities, strategies for locating the operator, and recommended safety procedures if the device lands on the field or in the stands.

In addition, the NFL has increasingly engaged the Federal Aviation Administration and other policymakers on the development of new policies, procedures, and approaches related to reducing the threat posed by drones. We support the Federal Aviation Administration's efforts to adopt and implement a remote identification requirement for all, or nearly all, drones sold or operated in the United States. Federal officials, air traffic control operators, and local law enforcement officers need a simple and easy method to identify a drone and its operator when a device is spotted in a dangerous location or in violation of an established flight restriction. Any class of drones excluded from such a requirement must be very narrow and limited to drones that do not present any possible security threat to a large gathering of people. In addition, for the FAA to implement such a robust remote identification requirement, Congress must revise the hobbyist exemption in section 336 of the FAA Modernization and Reform Act of 2012. Although this provision was undoubtedly well intentioned at the time it was adopted, it is too broad for today's environment. The current hobbyist exemption permits far too many drones to be flown by far too many unlicensed and untrained pilots. As I noted earlier, the vast majority of the incursions at NFL stadiums are by such hobbyists.

Further, we supported the aims of S. 2836, the Preventing Emerging Threats Act of 2018, which would extend drone interdicting authority to the Department of Homeland Security and the Department of Justice. The bill represents an important step forward in helping to provide greater protections of our homeland.

Under the legislation, the Department of Homeland Security would be required to conduct research, testing, training, and evaluation of counter-drone equipment. This will promote and accelerate technologies that will help law enforcement identify, mitigate, and interdict illicit or hostile drones that threaten security, including in environments that present geographic challenges – such as densely populated, urban areas.

The bill also provides federal law enforcement officials at the Department of Homeland Security and the Department of Justice the authority to take the necessary steps to mitigate and counteract the threat posed by drones in certain circumstances. Such circumstances include when a governor or state attorney general requests that federal law enforcement officials provide support for state, local, or tribal law enforcement to ensure the security of mass gatherings. This provision correctly recognizes that local law enforcement officers stand at the frontlines and are primarily responsible for providing safety and security at locations where drones present risks, including large amateur and professional sporting events, such as NFL games.

Importantly, however, this provision only permits local officials to request assistance from federal officials, and experience has taught us that there simply are not enough federal resources and personnel to provide security at all events that need protection, including the 256 NFL games that occur across the country in a season. For example, the Department of Homeland Security reviews between 12,000 and 15,000 events annually for a Special Event Assessment Rating (SEAR), and the Department has historically approved fewer than 20 events annually for SEAR 1 or SEAR 2. Notably, the Super Bowl has been a SEAR 1 event.

In my experience in Washington after the September 11 terrorist attacks, I observed a similar challenge – there simply were not enough federal resources to handle the significant increase in antiterrorism initiatives and activities. After September 11, we were able to solve that problem by expanding our use of joint terrorism task forces. The task forces permitted local law enforcement officials to exercise authorities as if they were federal officials. We need a similar approach to drone interdiction authorities.

The NFL, therefore, believes that expanding federal drone interdiction authority is an important step, but it is insufficient to address the security needs of the NFL in protecting our stadiums and fans from the threat posed by drones. The NFL strongly encourages Congress to consider additional reforms that would provide authorities to local law enforcement officers, with appropriate training and expertise, to detect and intercept drones that pose a known and identifiable threat to an NFL game in violation of the flight restrictions that Congress and the Federal Aviation Administration have established. Additional reforms could include the following:

- Permit the Attorney General or the Secretary of Homeland Security to delegate drone countermeasure authorities to state and local law enforcement protecting a large sporting event covered by a temporary flight restriction.

- Require the Attorney General and the Secretary of Homeland Security to consult with state and local law enforcement, and incorporate state and local law enforcement personnel into the implementation of drone countermeasure programs.

- Establish a pilot program to include state and local law enforcement personnel in the programs developed pursuant to the legislation.

The NFL looks forward to continuing to work with Congress, the Federal Aviation Administration, and others on our shared goal of ensuring the safety and security of the players, coaches, fans, and staff who attend our games. Thank you for the opportunity to be here today, and I would be pleased to answer your questions.

STATEMENT of
MR. SCOTT A. McBRIDE
INFRASTRUCTURE SECURITY MANAGER
NATIONAL & HOMELAND SECURITY
IDAHO NATIONAL LABORATORY

BEFORE THE

UNITED STATES SENATE
HOMELAND SECURITY & GOVERNMENTAL AFFAIRS COMMITTEE

September 13, 2018

Mr. Scott A. McBride, Infrastructure Security Manager, National & Homeland Security, Idaho National Laboratory

U.S. Senate Hearing to receive testimony on "Evolving Threats to the Homeland"

Chairman Johnson, Ranking Member McCaskill, and distinguished members of the committee, thank you for holding this hearing and inviting Idaho National Laboratory's testimony on the potential threat of Geomagnetic Disturbance (GMD) and Electromagnetic Pulse (EMP) to the U.S. power grid. I greatly appreciate the opportunity to address this committee and thank the members for your interest in discussions of the risks these threats represent, and your dedication to develop legislative decisions that will assure that our national energy supply is reliable, resilient and protected.

I request that my written testimony be made part of the record.

I am the Infrastructure Security Manager for National and Homeland Security at Idaho National Laboratory, also known as INL. INL is one of 17 the U.S. Department of Energy (DOE) national laboratories and is the nation's lead nuclear energy laboratory. INL's mission is to conduct research, development and demonstration of solutions that will assure the advancement of nuclear energy, clean energy, and critical infrastructure protection technologies – all with the objectives of assuring the energy, economic, and national security of the U.S. In my role at INL, I have the pleasure and responsibility to lead, influence, and execute research, development, testing, demonstration, and deployment of technology as it applies to securing our nation's critical infrastructure, with an emphasis on the energy sector. My background includes a balance of experiences with development and operations of grid infrastructure for public electric utilities, and power engineering research and testing of security technologies on a unique, full-scale test grid at the INL site. I am one of the principle investigators and test designers for the nation's seminal research of the scientific principles and impacts of geomagnetic disturbance ground induced currents on electrical substations and downstream electrical equipment.

The U.S. electric power grid incorporates new digital technology with legacy infrastructure that can be decades old. This combination results in a grid that is vulnerable to GMD and EMP events, whether the EMP source is from nuclear or non-nuclear sources. The vulnerability of the grid to EMP is due to potential damage to the individual components and the larger, massively interconnected electric generation, transmission & distribution systems, and the breadth of uncertainties of the effects caused by the three waveforms identified by their different magnitude, durations, and interdependencies during an EMP event. E1 and E2 waveforms can couple with long power lines, transmitting thousands of amperes of current to connected systems tens of miles away. This can disable electrical and electronic systems through permanent thermal damage to components or upset to digital electronics. The E3 waveform's associated harmonics and impedance mismatches can damage equipment, including large substation transformers, uninterruptible power supplies, long-haul communications, and possibly generators. GMD causes similar effects to E3. Currently, there is a fairly robust understanding of the scientific principles of E1 and E2 that enable us to predict effects and design protections. Initial experiments have been completed and models are beginning to emerge that assist us in better understanding and characterizing effects and impacts from E3. Research and testing of the interdependent effects of the combined three waveforms on our grid's individual components and interconnected infrastructure is an uncharacterized field of study that needs further exploration and discovery.

At present, the North American Electric Reliability Corporation's (NERC's) Emergency Preparedness and Operations (EOP-10-1) and Transmission Planning (TPL-007) are standards issued that deal exclusively with protection of the electric power grid from a GMD event - not the full range of threats posed by an EMP event and its concurrent waveforms.. My current understanding of the science, and the results of my experiments and tests of developmental protective technologies lead me to a position that – relying on the current industry electric grid protections, based on standards for lightning and GMD protections, leave the grid inadequately protected against the effects of EMP. While existing grid standards may partially alleviate E2 and E3 effects, the grid remains unprotected against the high amplitude, fast rise time characteristics of an E1 pulse.

The Nation's High Voltage (HV) and Extra High Voltage (EHV) power grid contains a few thousand large power transformers which are potentially vulnerable to the threat of GMD events. These transformers are very expensive to build and typically have long lead times of 18 to 24 months. EHV transformers are not currently manufactured in the U.S., and industry maintains very few critical spares. GMD events drive HV and EHV transformers into heavy half-cycle saturation that then induces voltage harmonics in power systems which can cause damage to power system components and loads. The induction of quasi-Direct Current (DC) in power systems can also be caused by the "Blast" and "Heave" portions of the EMP E3 from a nuclear device detonated above 80 kilometers altitude.

A mature, tested and validated technology has been developed and represents one potential solution to protect HV and EHV power transformers from the threat of both GMD's and EMP's. The EMP hardened transformer Neutral Blocking Device (NBD) is designed to provide automatic protection for HV and EHV transformers against GMD and EMP events - when GMD or EMP induced currents in a transformer are detected. The device provides a metallic path to solidly ground the transformer during normal operation and an Alternating Current (AC) effective grounding path for the transformer for only short periods (i.e. a few minutes to hours) when a solar disturbance (GMD) or an EMP event is impacting the earth. Power grid modeling and studies have shown that neutral blocking in a power grid provides significant reductions in reactive power (VAR) consumption and Ground Induced Current (GIC) harmonics as well as protection against protective relay mis-operations. Additionally, NBD's enhance the protection of Generator Step-Up (GSU) transformers at hydro-generation facilities which can provide important black-start resources for a power grid.

Even with the NBD's, the "Blast" and "Heave" portions of the EMP E3 pose a direct threat to the large power transformers that our country depends on and is not yet equipped to replace.

Hence, it can be implied that there must be a priority to protect the most critical large power transformers in place – my preliminary estimates are that this would cost less than $4 billion if we made it a priority to install NBD's at our most critical EHV substations. This is a small fraction of the value of replacement units, but more importantly is negligible compared to the loss of civilian life and long term recovery costs to the economy should they fail during a GMD or EMP event.

A basis for considering this approach is that in February 2015 the American Transmission Company (ATC) installed a NBD manufactured by ABB marketed as SolidGround™ in one of their substations in Wisconsin to improve power grid stability and protect against GMD's. This unit has operated and blocked GIC's as designed without issues during six (6) low-level solar storms (GMD's). SolidGround™ operates automatically and provides several monitoring signals to the Supervisory Control and Data Acquisition (SCADA) system through the substation control house. The experience to date has shown no signs of unintended consequences introduced into protective relays or other power system components. The device blocks GIC, prevents harmonic generation, reduces reactive (VAR) power demand and helps prevent voltage collapse during GMD events. Since this unit was placed in operation it operated over 30 times.

Beyond utilizing NBD's, I also advocate that we improve our capability to fully understand the extent of the vulnerability and reduce or eliminate consequences of GMD and EMP events. The Department of Energy recently tasked the national laboratories to develop a report that updates the extent of our current scientific understanding of the effects of EMP on the electric power grid. Pending this report's publication, significant progress for GMD and EMP grid protection can be made by pursuing three concurrent paths:

1) Define the E1-E2-E3 composite threat environment waveform, including coupled currents and voltages for transmission and distribution lines, in support of developing an informed 'all hazards' protective strategy;
2) Conduct a series of scaled experiments and tests on a variety of representative grid components and restoration assets to close the knowledge gap that affects our ability to understand, predict, and measure the impacts of GMD and EMP events on unprotected systems, as well as the effectiveness of all protective measure options.
3) Identify the priority infrastructure that can lead to a most effective and impactful set of actions that will harden the grid and enable reliable blackstart processes.

This set of targeted actions, with appropriate and coordinated government and private partnerships, can lead to a set of effective hardness and protective measures for GMD and EMP events that add quantifiable, cost-effective resiliency to the grid.

Defining the E1-E2-E3 composite threat environment waveform is needed to de-conflict integrated protection methods and to enable the development of future standards and design requirements for interoperable, all-hazard protection of the grid's digital components and interconnected systems. Research that can advance our understanding of the composite waveform will include determining whether our current understanding of the principles for modeling E1, E2, and E3 are also applicable for HEMP, GMD, and Radio Frequency Weapons

(RFW) environments. Additional research will be needed to further characterize differences well enough that models can be developed for simulating effects across all likely combinations of electromagnetic radiation environments. The results of this research will have most benefit if they are concurrently shared in the development of validation experiments, standards, and regulatory guidance.

Experimentation of effects from waveforms and recovery processes on utility-owned grid assets are impractical, especially if experimentation is needed to validate component and system performance during damaging or full-destructive test events. Hence, INL, along with some of our peer national laboratories, utilized DOE and other government investments in the design and construction of power grid test beds that can perform and recover from the needed experiments. Current gaps in knowledge suggest that the experiments of highest priority need to explore, and are not limited to: a) the propagating electromagnetic radiation effects to assets directly connected to long power lines, antennas, and communication/data lines; b) effectiveness of shielding, including non-conductive critical communication fiber, well-grounded equipment racks, and shielded buildings; c) effectiveness of developmental technologies for transient voltage surge suppression; and d) exercising high-voltage system operations and processes for critical system spares replacement, restoration procedures, and recovery processes. The results of this testing will have the most benefit if they are concurrently shared in the development of priorities for more research that can be utilized to enhance predictive models, and serve as the technical basis for standards, and regulatory guidance.

In balancing the rollout of digital technologies for assuring the cost-effective availability and reliability of the grid, with the sense of urgency to protect the electric grid from the effects of electromagnetic radiation, there is an opportunity to gain a significant level of protection by first focusing on deploying protective measures on the most critical assets for normal grid operation and recovery. Establishing a public-private partnerships allows for information sharing and threat analyses to assist asset owners in identification of the highest priority grid components and systems for protection to maintain electricity delivery and optimize recovery and restoration of services. With this information, a set of government validated credible threats can be evaluated with the research models to predict the effectiveness of protective technologies, design standards, and recovery processes. The integration of this information, including the holistic view of asset owners' vast knowledge and experience with their systems' designs, processes, operational data, and experience, can guide a prioritized series of investments in the installation and implementation of protections.

Even though the electric power grid is vulnerable, protection of the grid against the effects of GMD and EMP, though challenging, is possible. While it may not be plausible to protect all assets, careful prioritization of the implementation of protections can enable critical portions of the grid to survive, or at least be rapidly restored. Cooperation between government and industry will benefit the development of an optimal strategy for completion of the highest priority research and testing, legislative direction, regulatory guidance, engineering standards, and infrastructure modifications. Government and industry can accelerate full implementation of a protection strategy through a common technical understanding of the threat characteristics and system effects.

I thank the Committee's members for the opportunity to share my knowledge and leadership thoughts on the vulnerabilities and solutions for protection of the national power grid. I deeply appreciate the contributions of my fellow panel members' and your strong support for today's discussions. Today's hearing is a highly positive step towards enhancing our mutual understanding of the technical challenges of GMD and EMP threats to the grid, assuring that there is credible science and engineering basis supporting future legislative actions. You have my commitment to continue to obtain and share scientific knowledge as it gained and utilize that knowledge to advocate and pursue the development and testing of technical innovations that will resolve the threats of GMD and EMP.

Testimony before the U.S. Senate Committee on Homeland Security and Governmental Affairs
Hearing on "Evolving Threats to the Homeland"

September 13, 2018

Jennifer Bisceglie
CEO and President of Interos Solutions, Inc.

Chairman Johnson (R-Wis.), Ranking Member McCaskill (D-Mo.), and Members of the Committee, thank you for the invitation and opportunity to speak with you today on the underappreciated threats to the homeland that, if not mitigated, could significantly damage the nation's critical infrastructure and/or disrupt people's lives, especially as it relates to the global supply chain and the use of information and communications technology, or ICT.

By way of introduction, Interos is a company I founded over 13- years ago to evaluate risks in the global economy and the business partnerships, alliances and distribution networks that comprise our supply chains. Interos is built on my over 25 years in the global supply chain industry, having helped numerous US-based companies off-shore their manufacturing and take advantage of different skillsets, labor pools and competitive business arrangements with partners around the world.

During those years, I've watched risk concerns in the supply chain transition and grow from quality, to physical security, to resiliency and now to include product integrity. Interos recently supported the U.S.-CHINA ECONOMIC and SECURITY REVIEW COMMISSION for their report ('the Report") on Supply Chain Vulnerabilities from China in the U.S. Federal Information and Communications Technology (ICT) which outlines several recommendations, the most important being that the U.S. establish a "National Strategy for Supply Chain Risk Management (SCRM) in U.S. ICT" with supporting policies, so that the Nation's security posture is forward-leaning vs reactive and based on incident response. Our adversaries have strategies they are executing; it's my opinion this is missing in the U.S. and providing easy opportunities for nefarious actors to drive up risk exposure and cost.

In being invited here, today, I'd like to address six (6) areas that are directly related to the Report and remain highly relevant to this hearing's discussion. However, I would like to stress that whether it is 5G, blockchain, the Internet of Things (IoT), or any other emerging technology or threat, an underlying foundation for security is an understanding of who the stakeholders are across your business partnerships, alliances and distribution eco-systems, where your vulnerabilities lie, - what's most important - and having a comprehensive strategy for security and risk management.

Given its position in the market, Interos has had the opportunity to work with many public and private sector organizations across industries and the situation is always the same – if the organization's leadership doesn't take a focused and comprehensive approach to risk management - there will be unmanaged exposure and invariably negative impact.

The rest of my testimony is organized as follows:

- *A brief assessment of the emerging economic and national security risks from next generation connectivity and devices (particularly the IoT and 5G networks) for the U.S. with specific reference to the risks posed by other economies such as China, Russia and other sensitive countries. What* *additional risks, if any, does use of IT, standards, and/or equipment developed in sensitive countries pose to U.S. security? Are existing authorities and regulations adequate to address these challenges?*

- *How reliant are the U.S. government and U.S. IT firms on sensitive country firms and the IT products and services of those countries?*

- *What are the potential vulnerabilities from U.S. usage of sensitive country, China for example, IT, standards, and/or equipment?*

- *How, if at all, has the government of sensitive countries leveraged IT and IoT for the purposes of intelligence collection, censorship, or to launch or enable cyber-attacks? What are the implications for the integrity of U.S. government IT supply chains, for U.S. economic health, and for U.S. national security interests?*

- *Assess U.S. government's success in managing the risks associated with a company, and those products and services, from sensitive countries, to its IT procurement supply chains. How is the U.S. government seeking to address/mitigate its supply chain risks? How successful have those efforts been? What are the remaining challenges? Is existing legislation and regulations adequate to address these challenges?*

- *What steps should the U.S. government and U.S. Congress take to address the emerging security and economic risks from technology sourced from outside of the US?*

1. A brief assessment of the emerging economic and national security risks from next generation connectivity and devices (particularly the IoT and 5G networks) for the U.S. with specific reference to the risks posed by other economies such as China, Russia and other sensitive countries. What additional risks, if any, does use of IT, standards, and/or equipment developed in sensitive countries pose to U.S. security? Are existing authorities and regulations adequate to address these challenges?

Software supply chain attacks will become easier – and more prevalent - as developing technologies such as fifth generation (5G) mobile network technology and the IoT exponentially increase the avenues for attack.[1] Gartner predicts that by 2021 there will be 25.1 billion IoT units installed,[2] and by 2020, IOT technology will be in 90 percent of new computer-enabled product designs.[3] This growth in IoT connectivity will have a significant impact on the ICT SCRM challenge. Relevant to the Report, increasing IoT installations will expand the attack surface of federal ICT networks while decreasing the time required to breach them, yet to date, the time required to detect breaches is not decreasing. The

[1] The Internet of Things refers to a system of interrelated computing devices, mechanical and digital machines, objects, and living beings equipped with network connectivity that enables them to connect and exchange data.

[2] Peter Middleton, Tracy Tsai, Masatsune Yamaji, Anurag Gupta, Denise Rueb, "Forecast: Internet of Things — Endpoints and Associated Services, Worldwide, 2017," Gartner, Inc., December 21, 2017. https://www.gartner.com/doc/3840665/forecast-internet-things--endpoints.

[3] Benoit J. Lheureux, et al., "Predicts 2018: Expanding Internet of Things Scale Will Drive Project Failures and ROI Focus," Gartner, Inc., November 28, 2017. https://www.gartner.com/doc/3833669/predicts--expanding-internet-things.

responsibility of both the public and private sector in improving their approach to risk awareness and management in the commercial technology supply chain cannot be overstated.

The information technology (IT) supply chain threat to U.S. national security stems from products produced, manufactured, or assembled by entities that are owned, directed, or subsidized by national governments or entities known to pose a potential supply chain or intelligence threat to the U.S., including China, North Korea, and Russia. These products could be modified to 1) perform below expectations or fail, 2) facilitate state or corporate espionage, or 3) otherwise compromise the confidentiality, integrity, or availability of a federal information technology system.

In the past, this concern was exemplified by counterfeit components entering the supply chain of U.S. defense systems, such as counterfeit integrated circuits from China discovered in the U.S. Navy's P-8A Poseidon airplane, in a U.S. Air Force cargo plane, and in assemblies intended for Special Operations helicopters.[4] In 2011, the Senate Armed Services Committee investigated 1,800 cases of counterfeit components which created vulnerabilities throughout the Department of Defense's supply chain, and reported that 70 percent of all counterfeits come from China, and a majority of the remaining counterfeits could be traced back through the supply chain to China. In these cases, recycled, obsolete, or modified components passed off as genuine circuits had potential to perform below expectations or fail, threatening U.S. national security and the safety of U.S. service members.

Increasingly, the importance of an ICT component's physical structure pales in comparison with the firmware and software operating within it. In 2016, researchers identified vulnerabilities that allowed hackers to surveil and manipulate users by hacking the embedded firmware of their computer monitors.[5] In 2017, researchers uncovered vulnerabilities in printers manufactured by Hewlett-Packard, Dell, and Lexmark that allowed attackers to steal passwords, shut down printers, and even reroute print jobs.[6] The mid-2017 CCleaner supply chain attack, in which hackers accessed the code development structure of Piriform in order to install malware into the company's Windows utility product, typifies the types of threats federal ICT systems will continue to face. Over 2.2 million users downloaded CCleaner and unwittingly installed the hacker's embedded malware at the same time. This malware compromised 40 international technology firms, 51 international banks, and at least 540 computers connected to various governments.[7] Firms targeted by the hackers included many within the federal ICT ecosystem, including Cisco, Google (Gmail), Microsoft, Intel, Samsung, Sony, HTC, VMware, Vodafone, Epson, and Oracle.[8]

[4] U.S. Senate Committee on Armed Services, "Senate Armed Services Committee Releases Report on Counterfeit Electronic Parts," Press Release, May 21, 2012. https://www.armed-services.senate.gov/press-releases/senate-armed-services-committee-releases-report-on-counterfeit-electronic-parts.

[5] Lorenzo Franceschi-Bicchierai, "Hackers Could Break into Your Monitor To Spy on You and Manipulate Your Pixels," *Motherboard*, August 6, 2016. https://motherboard.vice.com/en_us/article/jpgdzb/hackers-could-break-into-your-monitor-to-spy-on-you-and-manipulate-your-pixels.

[6] Tom Spring, "Flaws Found in Popular Printer Models," *Threat Post*, January 31, 2017. https://threatpost.com/flaws-found-in-popular-printer-models/123488/.

[7] Lucian Constantin, "Researchers Link CCleaner Hack to Cyberespionage Group," *Motherboard*, September 21, 2017. https://motherboard.vice.com/en_us/article/7xkxba/researchers-link-ccleaner-hack-to-cyberespionage-group.

[8] India Ashok, "CCleaner Hack: Chinese Hacker Group Axiom May Have Carried out Attack to Target Major Tech Giants," *International Business Times*, September 21, 2017. http://www.ibtimes.co.uk/ccleaner-hack-chinese-hacker-group-axiom-may-have-carried-out-attack-target-major-tech-giants-1640208; Catalin Cimpanu, "Avast Publishes Full List of Companies Affected by CCleaner Second-Stage Malware," *Bleeping Computer*, September 25,

As information technology advances, and connectivity increases, these risks will multiply. Concepts such as the IoT, are but one avenue by which risk to federal IT systems will increase. The National Institute of Standards and Technology stated in Draft NISTIR 8200, released in February 2018, that "the adoption of IoT brings cybersecurity risks that pose a significant threat to the Nation."[9] Other aspects of supply chain risk depend on technologies that are not yet fully developed or deployed, such as 5G mobile network technology, which is expected to start deploying in 2020. The full deployment of 5G networks is expected to dramatically expand the number of connected devices, reduce network energy use, and decrease end-to-end round trip delay (latency[10]) to under one millisecond.[11] 5G is important for subsequent developments in virtual reality, artificial intelligence, and seamless integration of IoT.[12,13] Faster connectivity supplied by 5G networks will enhance productivity, efficiency, and facilitate greater interconnectedness through the IoT. But these benefits come with increased cybersecurity risks.

What additional risks, if any, does use of IT, standards, and/or equipment developed in China pose to U.S. security?

The Chinese government and Chinese firms are hoping for a larger stake in the new 5G developments than they had in 3G and 4G-LTE.[14] Key decisions on these standards will be made in international organizations such as the International Telecommunication Union (ITU) and the Third Generation Partnership Project (3GPP). The ITU is a specialized agency of the United Nations responsible for ICT issues; the 3GPP is a collaborative organization among telecommunications associations. In both arenas, China has sought leadership positions to increase its influence. In the 3GPP, China has been represented by members of Huawei and China Mobile. In October 2014, Houlin Zhao was elected secretary general of the ITU.[15] His four-year term began January 1, 2015 and concludes at the end of 2018.

Although the finalization of 5G standards may be years away, Chinese entities (specifically Huawei and ZTE) have made large strides in patenting ICT innovations, and China could emerge as an industry leader

2017. https://www.bleepingcomputer.com/news/security/avast-publishes-full-list-of-companies-affected-by-ccleaner-second-stage-malware/; Dan Goodin, "CCleaner Backdoor Infecting Millions Delivered Mystery Payload to 40 PCs," *Ars Technica*, September 25, 2017. https://arstechnica.com/information-technology/2017/09/ccleaner-backdoor-infecting-millions-delivered-mystery-payload-to-40-pcs/.

[9] National Institute of Standards and Technology, *Draft NISTIR 8200 Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things (IoT)* (Gaithersburg, MD: Computer Security Division, February 2018). https://csrc.nist.gov/CSRC/media/Publications/nistir/8200/draft/documents/nistir8200-draft.pdf.

[10] Latency refers to the delay before a transfer of data begins following an instruction for its transfer. Decreasing latency to under one millisecond is seen as vital to successfully developing safe self-driving vehicles and producing virtual reality programs that can deliver data at a rate that feels near-instantaneous to humans.

[11] Jo Best, "The Race to 5G: Inside the Fight for the Future of Mobile as We Know It," *TechRepublic.* https://www.techrepublic.com/article/does-the-world-really-need-5g/.

[12] The Internet of Things refers to a system of interrelated computing devices, mechanical and digital machines, objects, and living beings equipped with network connectivity that enables them to connect and exchange data.

[13] Sebastian Moss, "ITU and Huawei Call for Government-backed Broadband Investment," *Data Center Dynamics*, October 7, 2016. http://www.datacenterdynamics.com/content-tracks/core-edge/itu-and-huawei-call-for-government-backed-broadband-investment/97066.fullarticle.

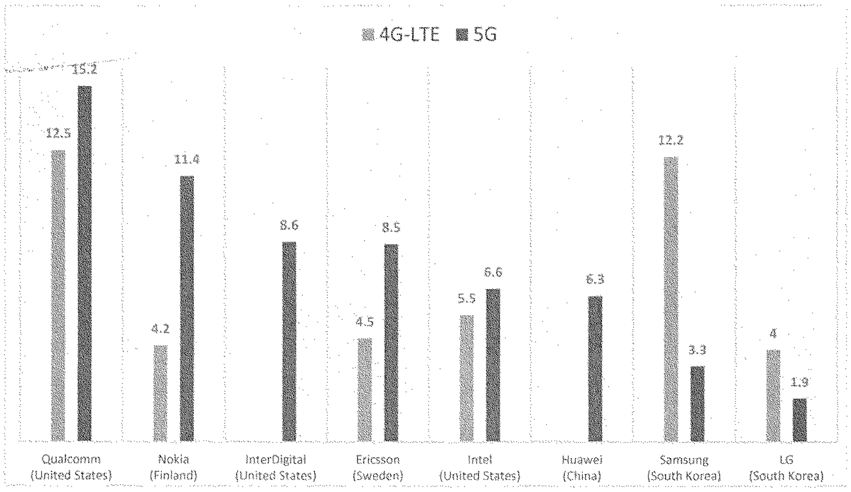
[14] 4G-LTE, or long-term evolution is a telecommunication standard for high-speed wireless communication for mobile devices and data terminals.

[15] "Biography—Houlin Zhao," International Telecommunication Union, 2017. http://www.itu.int/en/osg/Pages/biography-zhao.aspx; Xinhua, "China's Zhao Houlin Elected as Secretary-general of ITU," *China Daily USA*, October 23, 2014. http://usa.chinadaily.com.cn/world/2014-10/23/content_18791007.htm.

in this technology.[16] Of the 4,123 patents that ZTE applied for in 2016, more than 1,500 are 5G-related.[17] Huawei's 5G research dates to 2009 and includes advances in polar coding and network splicing routers. Huawei has also bought technology patents from Sharp, IBM, Siemens, Harris Corporation, and other U.S., Japanese, and European companies. These patent acquisitions focus on communication technologies such as the Session Initiation Protocol.[18]

A March 2017 report by LexInnova laid out the major players in the 5G network technology IP landscape.[19] **Exhibit 7** of the report shows the share of 4G-LTE and 5G IP among top firms. Qualcomm, Nokia, InterDigital, Ericsson, Intel, and Huawei are the top six firms for 5G IP. Qualcomm, Samsung, Intel, Ericsson, Nokia, and LG were the top six firms for 4G-LTE IP. Many of the top firms from 4G-LTE development remain competitive in the 5G sphere, with Qualcomm continuing to lead the group, and Nokia, Ericsson, and Intel increasing their share of relevant IP rights in 5G with respect to 4G-LTE. Although Samsung was a close second to Qualcomm in 4G-LTE innovation, it has fallen to 10th in 5G IP, according to the LexInnova data. LG has similarly struggled, losing influence in 5G innovation to its competitors. Newly important players include InterDigital (a nonparticipating U.S. entity that owns IP but does not produce products) and Huawei.

Exhibit 7: Percent Share 4G-LTE and 5G Wireless Network IP Rights by Firm



[16] Ben Sin, "How Huawei Is Leading 5G Development," *Forbes*, April 28, 2017. https://www.forbes.com/sites/bensin/2017/04/28/what-is-5g-and-whos-leading-the-way-in-development/#1d015f0e2691.
[17] Saleha Riaz, "ZTE, Huawei Top Patent Application Table in 2016," *Mobile World Live*, March 16, 2017. https://www.mobileworldlive.com/featured-content/top-three/zte-huawei-top-patent-application-table-in-2016/.
[18] Jack Ellis, "A Peek Inside Huawei's Shopping Basket Reveals How Patent Purchases Further Its Expansion Plans," IAM, May 7, 2015, http://www.iam-media.com/Blog/Detail.aspx?g=0351e5a1-3675-43a9-a552-7c8206af6be3.
[19] LexInnova, "5G Mobile Network Technology: Patent Landscape Analysis," March 15, 2017. http://www.lex-innova.com/resources-Reports/?id=67.

Sources: LexInnova, iRunway, Jefferies.

According to the LexInnova data, Huawei may control as much as 6.3 percent of critical 5G mobile network technology IP, a shift from its lack of influence in 4G-LTE. All Chinese entities together (including contributions from Huawei, ZTE, the China Academy of Telecommunications Technology, Zhejiang University, and Lenovo Group) control 9.8 percent of the IP LexInnova deemed critical to the 5G standard. Chinese firms have the largest presence in the Radio Front End/Radio Access Network category, where Huawei has 41 patents, China Academy of Telecommunications Technology has 14, ZTE has 11, and Zhejiang University has 10. In the area of Modulation/Waveforms, Huawei has 27 patents, while Lenovo Group has 7. In the area of Core Packet Networking Technologies, Huawei has 24 patents and ZTE has 8. However, Chinese entities still lag behind ICT powerhouses such as Ericsson, Qualcomm, and Nokia, which represent the bulk of 5G-related patent holders.[20] The LexInnova report notes that the presence of Chinese entities among the top IP assignees may indicate that China's 5G deployment timeline is similar to that of the U.S.

Are existing authorities and regulations adequate to address these challenges?

In short, the answer is 'no'. An example is the recently implemented Modernizing Government Technology Act (MGT Act), introduced by U.S. Representative Will Hurd (R-TX), chairman of the House Information Technology Subcommittee, in September 2016. The Act creates a $500 million central modernization fund against which agencies can borrow to update aging IT systems. The Act also creates working IT capital funds that allow agencies to retain savings achieved from ongoing modernization efforts, provided they are used for future modernization projects. The Bill was amended to the Senate version of the FY18 National Defense Authorization Act, which was passed by Congress in November 2017 and signed into law on December 12, 2017.

The MGT Act seems to presume that legacy equipment and systems are the primary source of risk, and that this risk can be mitigated through modernization. But modernization will increase risk if newly adopted technologies, which have stronger supply chain connections to China, Russia, North Korean, Iran, Israel and other sensitive countries, are not assessed appropriately before being integrated into federal IT networks. The Bill establishes responsibilities and provides financial rewards to agencies for modernizing their IT infrastructure, naming OMB and GSA as permanent members of a supervisory board. However, it does not require any measure of supply chain security as part of modernization efforts. In the 'Implementation of the Modernizing Government Technology Act' signed by Director Mick Mulvaney on February 27, 2018, there are multiple pages of guidelines for the execution of the program, but no requirement for SCRM as part of an Agency's modernization effort.

An understanding of emerging technologies, their pedigree, and their interconnectivity is crucial to proactively identify and mitigate future supply chain risk to federal ICT systems. The Chinese government and Chinese companies have developed joint strategies to influence future developments to the advantage of Chinese ICT products. China's role in setting international technology standards is likely to increase, and similar strategies are likely to be used in the future in fields beyond ICT, such as pharmaceuticals, biotechnology, medical technology, nanotechnology, virtual reality, and artificial intelligence. Until U.S. leadership takes this vulnerability seriously, it will remain an 'easy button' for our adversaries.

[20] Guy Daniels, "If You Thought Patents Got Ugly with LTE, Just Wait until 5G," *Telecom TV.* http://www.telecomtv.com/articles/5g/if-you-thought-patents-got-ugly-with-lte-just-wait-until-5g-13458/.

2. How reliant are the U.S. government and U.S. IT firms on sensitive country firms and sensitive country-made IT products and services?

Over 95 percent of all electronics components and IT systems supporting U.S. federal IT networks are commercial off-the-shelf (COTS) products, and China's role in this global supply network is significant. The supply chain for civilian IT is a global enterprise dominated by suppliers in East Asia.[21] In addition to Chinese firms, many companies headquartered in Taiwan and Singapore base their manufacturing operations primarily in China. China assembles most of the world's consumer and commercial electronic devices, produces parts such as flash cards, and dominates the world in volume of IT industrial capacity. A recent report from the Government Accountability Office (GAO) noted that China is the largest importer and exporter of IT hardware globally, as well as a key manufacturing location of workstations, notebook computers, routers and switches, fiber optic cabling, and printers.[22]

Many of the top enterprise IT providers to the U.S. government are also among the largest manufacturers of federal ICT equipment, including leading providers of COTS products, such as Hewlett-Packard, IBM, Dell, Cisco, Unisys, Microsoft, and Intel.[23] Their supply chain is potentially influenced by China due to the fact that many of the companies and/or their sub-tier suppliers have manufacturing locations there.

China is not the only country the U.S. is concerned about, but their economic decision to invest in being the world's technology manufacturer should prioritize them.

3. What are the potential vulnerabilities from U.S. usage of sensitive country, China for example, IT, standards, and/or equipment?

The Chinese government considers the ICT a "strategic sector" in which it has invested significant state capital and influence on behalf of state-owned ICT enterprises. Since 2013, China has accelerated its efforts at indigenous production and independence in ways that have created a more restrictive environment for companies doing business in China, extracting concessions from large multinationals in exchange for market access.

New policies requiring companies to surrender source code, store data on servers based in China, invest in Chinese companies, and permit the Chinese government to conduct security audits on its products open federal ICT providers—and the federal ICT networks they supply—to Chinese cyberespionage efforts. China also continues to directly target U.S. government contractors and other private sector entities as part of its efforts to gain economic advantage and pursue other state goals.

[21] Danny Lam and David Jimenez, "US' IT Supply Chain Vulnerable to Chinese, Russian Threats," *The Hill*, July 9, 2017. http://thehill.com/blogs/pundits-blog/technology/341177-us-it-supply-chain-vulnerable-to-chinese-russian-threats.

[22] U.S. Government Accountability Office, "State Department Telecommunications: Information on Vendors and Cyber-Threat Nations," *GAO-17-688R State Department Telecommunications*, July 27, 2017. https://www.gao.gov/assets/690/686197.pdf.

[23] "Top 25 Enterprise IT Providers to Government," *FedScoop*, August 30, 2017. https://www.fedscoop.com/federal-it-top-25/federal-it-top-25-full-list/.

Specific risks include intellectual property theft, theft of Personally Identifiable Information of U.S. citizens that can be used for financial gains, and the insertion of counterfeit products and services meant to create disruption and do harm.

The use of Chinese standards further complicates any security strategy the U.S. may have in place as it provides a documented path of access for our adversaries.

How will the deployment of 5G and greater usage of IoT affect these vulnerabilities?

These new emerging technologies are just two (2) more examples that need to be proactively evaluated through a security lens as part of a national supply chain risk mitigation strategy. These, and other emerging technologies will expand the attack surface and increase the potential vectors for opportunists.

4. How, if at all, has the government of sensitive countries leveraged IT and IoT for the purposes of intelligence collection, censorship, or to launch or enable cyber-attacks? What are the implications for the integrity of U.S. government IT supply chains, for U.S. economic health, and for U.S. national security interests?

There are multiple documented examples of the sensitive countries' governments leveraging IT for intelligence collection and economic and state espionage efforts. One of the most infamous is probably the breach of Office of Personnel Management's database in 2015, a mammoth break-in that exposed the records of more than 22 million current and former federal employees.

In 2014 and 2015, the Chinese government ramped up implementation of laws and policies that raise market access concerns among ICT manufacturers and suppliers in the U.S. by threatening to decrease competition, favor Chinese firms over foreign firms, or extract concessions from multinational firms seeking to do business in China. These new regulations present a serious dilemma for U.S. multinationals and a threat to U.S. national security. If U.S. multinationals fail to adhere to Chinese government regulations, they may face restricted market access in China, which could decrease their revenues and global competitiveness. But if U.S. companies—which are the primary providers of ICT to the U.S. federal government—surrender source code, proprietary business information, and security information to the Chinese government, they further open themselves and federal ICT networks to Chinese cyberespionage efforts.

Bottom line, we need our full defenses up at all times to thwart enemy attacks.

5. Assess the U.S. government's success in managing the risks associated with sensitive country-firms and the products and services supplied, to its IT procurement supply chains. How is the U.S. government seeking to address/mitigate its supply chain risks?

A challenge facing federal SCRM efforts is that federal government laws and policies do not address risk management comprehensively. Rather, supply chain risks to federal ICT systems has been divided in multiple ways— among federal information systems and other initiatives designed to protect critical infrastructure or high-value assets and among national security systems (NSS) as a subset of federal information systems.

How successful have those efforts been? What are the remaining challenges?

In some instances, very impactful. Interos supported one federal agency where over 75% of the supply chain risk assessments conducted in the past three (3) years have identified concerns that altered acquisition decisions or influenced market analysis. That said, this mature program is in the minority when compared to those of other agencies where such programs exist. Not to mention, there are agencies that have not been resourced to implement a SCRM program at all. And, more importantly, as the Chief Information Officer (CIO) of that agency changed from a permanent to a political position, and this administration has not taken a strong stand on SCRM, the CIO cancelled the VERY SUCCESSFUL six-year running program. We were four (4) days from contract renewal and no reason for program cancellation was provided.

In the current supply chain risk ecosystem, responsibility for risk management is held at different levels within agencies. This often results in offices and lines of effort in several agencies that function largely as under-resourced stovepipes lacking in executive sponsorship or oversight, and catering to the needs and procurement policies of individual clients. The DoD and the intelligence community maintain largely separate policies, many of which are not transparent to or applicable to the broader federal government due to procurement practices and classification concerns, among other reasons.

6. Is existing legislation and regulations adequate to address these challenges?

In short, no. There is little to no priority placed on SCRM, minimal leadership involvement and limited accountability. I do not know what it will take to get this level of attention or how many other incidents need to occur before Congress or the Executive Branch gets more involved, but I see this as a major flaw in U.S. national security. At the same time, I would like to commend the agencies that have taken their own initiative to set up programs for internal security reasons – they are making a difference, but unfortunately these models are not scalable or shareable in their current form.

7. What steps should the U.S. government and U.S. Congress take to address the emerging security and economic risks from technology sourced from outside of the U.S.?

As previously mentioned, the Federal ICT supply chain risks can be best managed by focusing on four (4) areas: 1) embracing an adaptive SCRM process, 2) promoting supply chain transparency, 3) centralizing federal ICT SCRM efforts, and 4) crafting forward-looking policies.

This concludes my testimony. I thank the Committee and I would be pleased to answer your questions.

Post-Hearing Questions for the Record
Submitted to Kevin Mandia
From Senator Claire McCaskill

"Evolving Threats to the Homeland"

September 13, 2018

Supply Chain Risk Management

1. **Have you been tracking the recent supply chain conversations?**

Yes, FireEye has been tracking the recent supply chain conversations. Specifically, the FireEye Federal team has had meetings and interactions with several Federal organizations that have been looking for ways to improve the security of their supply chains. We are also aware of the more general comments, articles, and papers found throughout the Federal ecosystem.

What recommendations do you have for Congress to position the government so it can manage supply chain risk?

FireEye would offer the following recommendations for Congress:

- Maintain a broad definition of "supply chain" so as to encompass multiple facets, including but not limited to, elements such as computer components, software, the information contained within the networks and computer systems of federal contractors and sub-contractors. Small sub-contractors, particularly in the defense industrial base, present a significant risk, given that such entities often are forced to devote fewer resources to cybersecurity. As several recent episodes have proven in both the commercial and government spaces, these smaller entities can be highly vulnerable to attack and can serve as the attacker's point of entry into the larger enterprise.
- Define and publish the desired outcomes it seeks with respect to supply chain security.
- Plan for the incremental expense of the new/incremental security controls necessary to achieve its stated supply chain security outcomes.
- Seek to understand any changes that may be necessary to the legal and contractual framework that surrounds Federal contracting.
- Seek to fully understand, and manage, the fundamental tension between the highly competitive nature of Federal contracting and the need to implement adequate supply chain security controls.
- Direct NIST to review, and update as necessary, all Supply Chain Risk Management-related documents, including NIST 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, as an example.

We'd also generally suggest greater government-industry collaboration regarding the cyber threats facing the supply chain of the National Industrial Base (NIB), including:

- Increased information sharing from the government to the private sector on insider threats;

- Advanced sensor capabilities that can detect nation-state cyber threats to the NIB; Broader reliance on industry-leading capabilities for security automation, orchestration and response to combat cyber threats; and
- Formation of a joint government-industry fusion cell that combines the capabilities of the world's leading cybersecurity companies and the U.S. government to combat threats to the NIB.

2. **In your opinion, what is the government doing well regarding supply chain risk management and where do you believe the government needs to step up its game?**

The actions that the government has already taken, such as NIST 800-161 and NIST 800-171, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, are to be commended. The current dialog and action already taken by leaders throughout the government should also be positively recognized, including the Defense Department's latest security initiative to "Deliver Uncompromised," which includes security as a fourth evaluation criterion for making awards. The government should consider evaluating the ideas, concepts and recommendations set forth in that initiative and apply it to the entire federal government. Creating incentives for federal contractors to include security as part of a solution from the onset will help the government minimize risk and cost for possible future attacks on the entire National Industrial Base.

Information Operations

Last month, Facebook announced that it discovered some campaigns on its platform exhibiting "coordinated inauthentic behavior." Facebook removed 652 pages, groups and accounted that originated in Iran and targeted people across multiple internet services in the Middle East, Latin America, U.K. and the U.S.[2] Facebook noted that FireEye provided Facebook with a tip that helped them identify the campaigns.

3. **Please tell us more about the work FireEye is doing in that space, how it discovered the campaign, and the platforms on which FireEye is seeing this type of behavior.**

FireEye's intelligence division has a dedicated Information Operations intelligence analysis team that focuses on identifying these types of foreign influence campaigns. The team is made up of various language, regional, and geopolitical experts that combine traditional intelligence analysis with data analytics to identify and attribute influence campaigns leveraging malicious cyber threat activity or concerted, inauthentic online behavior. The Iranian operation is only one set of activity the team has uncovered and continues to track. Most prominently, the IO team continues to investigate and uncover Russian influence and disinformation activity targeting the West.

In the case of the Iranian influence operation, we first discovered the campaign while tracking some unrelated disinformation activity. A social media account was spreading disinformation, and when we investigated what other accounts were following it, we identified a network of accounts pushing suspicious content from one of the inauthentic news sites, Liberty Front Press.

[2] *Taking Down More Coordinated Inauthentic Behavior,* Facebook (Aug. 21, 2018) (https://newsroom.fb.com/news/2018/08/more-coordinated-inauthentic-behavior/).

The content, which was heavily focused on Middle East politics, appeared inconsistent with the purported personas of the social media accounts promoting it, which adopted the identities of politically left-leaning American individuals. Investigating the Liberty Front Press site, we identified connections to Iran via WHOIS information, as detailed in the report. We were subsequently able to identify additional inauthentic news sites being promoted by these social media accounts, identify ties between those sites and Iran, and then identify additional clusters of related social media activity. We continued this cycle of unraveling new sites and social media activity to unmask the broader operation detailed in our report.

This type of behavior occurs across most, if not all, social media platforms, as well as via dedicated websites. As the purpose of these types of campaigns is to spread messaging and amplify narratives far and wide, the actors behind this type of activity will utilize any and all platforms that allow them to reach their target audiences.

4. **Are you seeing this information/disinformation operations type of behavior on the rise or is there just more awareness about it now, and do you have suggestions on how to stop it?**

It is difficult to quantify the full extent of this type of activity, but we suspect it is both: as the Iranian activity demonstrates, there are likely multiple actors paying attention to how this type of activity is evolving and assessing how they might use similar techniques to achieve their own particular political goals and agendas. At the same time, the greater awareness of this type of activity following Russia's 2016 US election interference campaign means that there are more people looking for this kind of activity, and as a result, more incidents of such activity being uncovered. We suspect such activity is both on the rise and there is a concurrent greater awareness of it that continues to lead to new discoveries of such operations.

One approach to stopping such activity is to identify such operations, acknowledge that they exist, and educate people, both policy makers and the general public, about what they look like and how they operate.

More specifically, the public would benefit if media platforms cooperated more closely with content creators to verify that content they propagate is original and unaltered. The looming threat of deepfakes—video and audio recordings altered using machine learning techniques and already easy enough for unskilled users to employ—will require that all parts of the media ecosystem with an interest in preserving the integrity and truthfulness of mass communications work together with one another on solutions now, before public trust is eroded. We have already seen instances of hostile foreign governments deploying this technology in support of information operations' campaigns, and of political leaders using it to tip an election or incite local anger. Government regulation could play a role preventing those threats from playing out in the United States by encouraging the adoption of appropriate technologies to detect and defeat deepfakes and verification of content provenance for media allegedly shared by major accounts, such as news outlets or "verified" celebrity accounts. Time is a factor—while deepfakes and related information operations' techniques are mostly easy for the naked eye to detect anomalies, our experts believe that situation could change in the next 18 to 24 months when it may no longer be possible for non-experts to distinguish between original and machine-altered video without these preventive measures in place.

Post-Hearing Questions for the Record
Submitted to Kevin Mandia
From Senator Rand Paul

"Evolving Threats to the Homeland"

September 13, 2018

1. **Some Members of Congress have expressed interest in passing federal data breach response legislation in the wake of high-profile data intrusion incidents at Equifax, the Office of Personnel Management, Target, and elsewhere. Some of the proposals that have been introduced would set an arbitrary timeline for public notification or other response activities (such as replacing affected computers) that must occur in the event a breach is detected. Some bills set that deadline at 30 days after detection, some only 15 days, and some as low as 72 hours.**

    - **Based on your observations and experience, please describe the potential impact to consumers and to businesses presented by these deadlines.**

A federal data breach notification standard should aim to strike an appropriate balance between over- and under-notification with respect to when the public should be informed about a data security incident. Given the many variables in play during an incident and the response period, Congress should avoid establishing a strict notification deadline; rather, the law should only require notification after an entity determines that the data breach could result in a significant risk of identity theft or financial harm. Public notification deadline requirements which are tied to detection rather than remediation can also alert an attacker that they were detected and could then hamper the incident response effort. This could result in a longer, more difficult, and more expensive remediation for an organization which could in turn result in more parties impacted by the data breach.

- **A recent FireEye report[1] notes that, on average, attackers had access for 101 days before detection in 2017. With this in mind, is detection time an ideal trigger for mandated response activity?**

Although response activities cannot begin prior to detection, there are many steps an organization can take to detect attacks sooner. Many organizations have begun investing in people, products, and services which enable them to identify an attacker earlier and limit the impact of the types of attacks that cannot be prevented. While response activities may drive these detection and hardening improvements, organizations need to be proactive. As you correctly note, FireEye's M-Trends 2018 report asserts that organizations appear to be getting better at self-identifying breaches, rather than relying on notification from law enforcement or other external sources. Internally identified incidents have a much shorter "dwell time" – that is, the

[1] https://www.fireeye.com/current-threats/annual-threat-report/mtrends.html

number of days from first evidence of compromise that an attacker is present on a victim's network before detection – than events identified by external sources. In turn, FireEye has found that shortening the dwell time is a key factor in mitigating the severity of cyberattacks. Although detection is certainly the trigger for incident response efforts, we do not believe that it would be the appropriate trigger under law for public notification. In many circumstances, certain variables will dictate that the time of detection is either an infeasible or impractical time to notify. Given these considerations, we believe that the time in which the entity determines that there is a risk of identity theft or financial harm, rather than dwell time, is a more appropriate trigger for public notification.

- **What other triggers should Congress consider to give victims more latitude to manage risk for consumers?**

We would recommend that the government implement/require a third-party review of the security controls selected and implemented to protect consumer information. The government should establish an accreditation process for this third-party review process and procedure; such an accreditation could, for example, be an extension to NSA's CIRA accreditation process provided to third party Incident Response Service Providers.

A federal data breach notification law should define "data breach" in such a way that it is clearly tied to unauthorized acquisition of sensitive personal information that causes a risk of identity theft or financial harm. This type of definition will allow victims of data breaches to distinguish between incidents that pose a true risk to the public and that therefore merit notification, and those that do not present a risk to consumers. Additionally, the notification should not be performed until effective remediation has occurred and the attacker no longer has access to an organization's environment.

Responses of Cathy Lanier to Questions for the Record
regarding the September 13, 2018 "Evolving Threats to the Homeland" Hearing
Senate Committee on Homeland Security and Government Affairs
Submitted: November 9, 2018

QUESTION RELATED TO SECTION 336

1. **The Federal Aviation Administration favors a repeal of Section 336 of the Federal Aviation Act of 2012. It is critical for law enforcement to be able to establish the link between a drone that is in flight with the ground-based operator in order to pursue the threat. The FAA has emphasized the importance of requiring registration, remote identification and observance of air space requirements for all drone operators. Do you support a Section 336 repeal?**

   Response: Yes, the National Football League supported a repeal or substantial modification of Section 336 of the FAA Modernization Act of 2012, which prohibited federal regulation of hobby or recreational use of drones. As I stated in my testimony at the hearing, as well as in my written statement for the committee's June 6 hearing on the Preventing Emerging Threats Act of 2018, the exemption for hobbyist drones provided in section 336 was too broad for today's environment, permitting far too many drones to be flown by far too many unlicensed and untrained pilots. According to the league's data and analysis, flights involving such hobbyist drones accounted for the vast majority of game-day incursions of the restricted airspace over NFL games during the past several years and present significant risks to the safety and security of our fans and stadium-goers.

   The league, therefore, was pleased that Congress recently passed the Federal Aviation Administration Reauthorization Act of 2018, which repealed section 336. The repeal paves the way for the Federal Aviation Administration to move forward with and implement a robust remote identification and tracking requirement for nearly all drones purchased and operated in the United States. We support new requirements that will give federal officials, air traffic control operators, and law enforcement a reliable and simple way to identify a drone and its operator when a device is spotted in a dangerous or restricted location. This ability will significantly reinforce and strengthen the security infrastructure and protections around our games.

QUESTIONS RELATED TO JOHNSON-McCASKILL BILL

2. **In light of the concerns that deployment of counter drone technology may pose without operational testing in real life environments, do you believe that the Johnson-McCaskill bill is the most promising solution at this time? And what additional assistance should DHS and DOJ be providing you right now?**

Response: The NFL shares the belief that S. 2836, the Emerging Threats Act of 2018, sponsored by Senator Ron Johnson (R-WI) and Senator Claire McCaskill (D-MO), represents a positive and promising step for advancing counter-drone technology. The bill includes a provision that requires the Department of Homeland Security (DHS) and the Department of Justice (DOJ) to conduct research, testing, training, and evaluation of counter-drone equipment, at a time in which counter-drone technology is rapidly advancing and becoming increasingly available. The League, therefore, was pleased and encouraged that Congress included this important provision in the recently passed FAA Reauthorization Act of 2018.

According to recent estimates, there are more than 200 available counter-drone products manufactured by more than 150 firms in over 30 countries throughout the world. These systems have capabilities ranging from radio frequency (RF) detection, RF jamming, spoofing, GPS jamming, to beaming lasers. However, the effects of counter-drone operations on manned aircraft systems, avionics, air traffic control systems and lawfully operated drone operations remain largely unclear or unknown in many cases. Given this uncertainty, the efforts of DHS and DOJ going forward to assess counter-drone technologies will further promote and accelerate the development and deployment of such technologies, and help law enforcement to determine the most effective technologies to identify, mitigate and interdict hostile or wayward drones in certain environments, including those that may present geographic challenges, such as the densely populated, urban areas where many of our NFL stadiums are located.

In addition, the league was pleased that the FAA Reauthorization Act included a number of provisions that recognize that local law enforcement officers have primary responsibility for providing safety and security at locations where drones present risks, including large amateur and professional sporting events, such as NFL games. For example, the Act requires the FAA to develop a comprehensive strategy for outreach to state and local governments, and to provide guidance for local law enforcement agencies and first responders identifying and responding to public safety threats posed by unmanned aircraft systems. The FAA also is required to develop a website containing resources for state and local law enforcement agencies and first responders regarding the public safety threats posed by drones. Moreover, the legislation includes an important provision initially provided in S. 2836, which allows the Secretary of the Department of Homeland Security or the Attorney General to work with state, local and tribal law enforcement officials "upon request of the chief executive officer of the State or territory" to protect mass gatherings from drone operations that pose a threat to the safety of people in attendance. This provision represents an opportunity for DHS and DOJ to provide additional assistance to and coordinate with state, local and tribal law enforcement officials on best practices to prevent an incident at stadiums or arenas. We, therefore, urge DHS and DOJ to provide such assistance and coordination to local law enforcement, and to seek input from sports organizations, and other groups associated with mass gatherings on the use and deployment of the authorities provided in the FAA Reauthorization Act, including the development, testing, and use of countermeasures for unmanned aircraft systems.

QUESTIONS RELATED TO SUPPORT FOR CRITICAL INFRASTRUCTURE OWNERS AND MASS GATHERING VENUE OPERATORS AND OWNERS

3. **What support and guidance do you currently receive from the Department of Homeland Security, the Department of Justice and the FBI, and the Federal Aviation Administration on how to handle the threat posed by drones?**

   Response: The league collaborates with the Department of Homeland Security, the Department of Justice and the FBI, the Federal Aviation Administration, and other agencies in a number of ways to address the security and safety risks related to hostile or wayward drones. The Department of Homeland Security provides periodic guidance related to counter-unmanned aerial systems (C-UAS) to the league through materials, such as advisories and bulletins as well as presentations. Specifically, the Department has provided the NFL and local law enforcement agencies with instructions related to how best to respond to potentially dangerous drone operations as well as guidance regarding legal considerations related to taking such countermeasures. The Department also provides guidance, information and resources related to responding to UAS-related threats in its online "First Responder Toolbox."

   The Federal Aviation Administration conducts trainings and symposiums around the country regarding issues related UAS and related safety concerns. In addition, at the request of the NFL, the FAA will work with the league, local law enforcement and other security personnel to conduct tabletop exercises. These exercises simulate a variety of potentially dangerous scenarios and emergency situations and ensure that, in the event of such an incident, first responders, law enforcement and other security officials work together in an efficient and coordinated manner.

4. **What law enforcement related working groups do you participate in the help owners of critical infrastructure and mass gathering venues to be more prepared to address this treat?**

   Response: I currently serve on the Homeland Security Advisory Council (HSAC), which provides the Secretary of Homeland Security with independent advice and recommendations to support decision-making on a broad array of homeland security operations and activities. During the next several months and years, HSAC will continue providing advice and counsel on the critical issues related to safely integrating unmanned aircraft systems into the national airspace, while at the same time protecting the safety and security of our homeland. As I stated in my testimony before the committee, I also serve on the Department of Homeland Security's Critical Infrastructure Partnership Advisory Council (CIPAC) Working Groups, playing a leading role in providing counterterrorism advice and recommendations related to large-scale sporting events and other mass gatherings. CIPAC was established to facilitate interaction and coordination between governmental entities and representatives from the community of critical infrastructure owners and operators.